

PATENT ABSTRACTS OF JAPAN

(11)Publication number :
(43)Date of publication of
application :

09-160492
20.06.1997

(51)Int.Cl.

G09C 1/00
H04L 9/32

(21)Application
number :

07-324908

(71)
Applicant :

**MATSUSHITA ELECTRIC
IND CO LTD**

(22)Date of filing :

13.12.1995

(72)
Inventor :

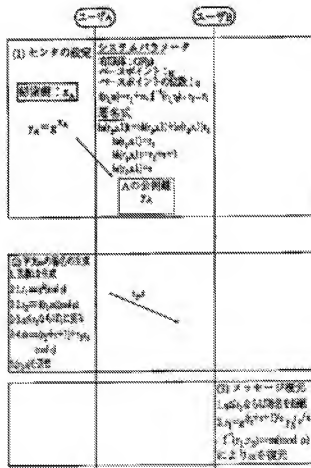
MIYAJI MITSUKO

(54) SIGNATURE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To attain a signature system capable of restoring a message and having high safety.

SOLUTION: Mapping (f) from $GF(p) \times GF(p)$ to $GF(p)$ satisfying following tow conditions to $GF(p)$ is set up as a message masking expression. In the 1st condition, three variables (t), (j), (e) are not replaced by two algebraic expressions in f (gtyAj, myAe) and f(gtyAj, mge) in the case of $GF(p)$ g, yA, m and $Zq=\{0, 1, \dots, q-1\}$ t, j, e. In the 2nd condition, the reverse image of $r2=f(r1, m)$ is $m=f-1(r1, r2)$. A signature expression is prepared by mapping ha, hb, hc from $GF(p) \times GF(p)$ to $GF(p)$ satisfying following expressions [1], [2] to $GF(p)$. Where, $hb(r2', s, 1)-ha(r2', s, 1) \neq hb(rr2', ss, 1)$ when $ha(r2', s, 1)=ha(rr2', ss, 1)$ and $hc(r2', s, 1)=hc(rr2', ss, 1)$ [1] and $hc(r2', s, 1)-ha(r2', s, 1) \neq hc(rr2', ss, 1)$ when $ha(r2', s, 1)=ha(rr2', ss, 1)$ and $hb(r2', s, 1)=hb(rr2', ss, 1)$ [2].



【特許請求の範囲】

【請求項1】 p を素数とし、有限体 $GF(p)$ の元を g とし、その位数を q とし、

$GF(p)$ 上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、

k を署名者が任意にとる乱数とし、 $r_1 = g^k \pmod{p}$ を署名生成処理におけるコミットメントとし、 $GF(p) \times GF(p)$ から $GF(p)$ への写像を f とするとき、 r_1 と m を f により変換した $f(r_1, m)$ を用いて署名生成処理におけるメッセージ復元を可能にするメッセージマスクを構成することを特徴としたメッセージ復元型署名方式。

【請求項2】 p を素数とし、 r を正整数とし、有限体 $GF(p^r)$ の元を g とし、その位数を q とし、 $GF(p^r)$ 上定義される署名方式において、署名したい文を $m \in GF(p^r)$ とするとき、 k を署名者が任意にとる乱数とし、 $r_1 = g^k \pmod{p}$ をコミットメントとし、 $GF(p^r) \times GF(p^r)$ から $GF(p^r)$ への写像を f_1 とし、 $GF(p^r)$ から有限環 $Z_{p^2} = \{0, 1, \dots, p^2-1\}$ への写像を π とするとき、 r_1 と m を f_1 により変換し、この値を更に π を用いて変換した $\pi(f_1(r_1, m))$ を用いて署名生成処理におけるメッセージ復元を可能にするメッセージマスクを構成することを特徴としたメッセージ復元型署名方式。

【請求項3】 p を素数とし、有限体 $GF(p)$ 上定義された楕円曲線を E とし、

$E(GF(p))$ の元を G とし、その位数を q とし、

$E(GF(p))$ 上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、

k を署名者が任意にとる乱数とし、 $R_1 = kG = (r_x, r_y)$ をコミットメントとし、

$E(GF(p)) \times GF(p)$ から $GF(p)$ への写像を f とするとき、 R_1 と m を f により変換した $f(R_1, m)$ を用いて署名生成処理におけるメッセージ復元を可能にするメッセージマスクを構成することを特徴としたメッセージ復元型署名方式。

【請求項4】 p を素数とし、 r を正整数とし、有限体 $GF(p^r)$ 上定義された楕円曲線を E とし、

$E(GF(p^r))$ の元を G とし、その位数を q とし、

$E(GF(p^r))$ 上定義される署名方式において、署名したい文を $m \in GF(p^r)$ とするとき、

k を署名者が任意にとる乱数とし、 $R_1 = kG = (r_x, r_y)$ をコミットメントとし、

$E(GF(p^r)) \times GF(p^r)$ から $GF(p^r)$ への写像を f_1 とするとき、 R_1 と m を f_1 により変換し、この値を更に π を用いて変換した $\pi(f_1(R_1, m))$ を用いて署名生成処理におけるメッセージ復元を可能にするメッセージマスクを構成することを特徴としたメッセージ復元型署名方式。

【請求項5】 写像 f は、 $GF(p) \ni g, y_A$ 及び m 、並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$ 及び e に対し、

$f(g^t y_A^j, my_A^e)$ 及び $f(g^t y_A^j, me^e)$ において、3変数 t, j, e が2個の代数式で非置換であることを特徴とした請求項1記載の離散対数問題を用いた署名方式。

【請求項6】 写像 f は、 $GF(p^2) \ni g, y_A$ 及び m 、並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$ 及び e に対し、 $f_1(g^t y_A^j, my_A^e)$ 及び $f_1(g^t y_A^j, me^e)$ において、3変数 t, j, e が2個の代数式で非置換であることを特徴とした請求項2記載の離散対数問題を用いた署名方式。

【請求項7】 写像 f は、 $E(GF(p)) \ni G$ 及び y_A 、 $GF(p) \ni m$ 、並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$ 及び e に対し、 $f(tG + j y_A, m \times x(e y_A))$ 及び $f(tG + j y_A, m \times x(eG))$ において、3変数 t, j, e が2個の代数式で非置換であることを特徴とした請求項3記載の離散対数問題を用いた署名方式。

【請求項8】 写像 f は、 $E(GF(p^r)) \ni G$ 及び y_A 、 $GF(p^r) \ni m$ 、並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$ 及び e に対し、 $f(tG + j y_A, m \times x(e y_A))$ 及び $f(tG + j y_A, m \times x(eG))$ において、3変数 t, j, e が2個の代数式で非置換であることを特徴とした請求項4記載の離散対数問題を用いた署名方式。

【請求項9】 写像 f は、 $GF(p) \ni r_1, r_2, m, g$ 及び y_A に対し、 $r_2 = f(r_1, m)$ の逆像を $m = f^{-1}(r_1, r_2)$ で定義するとき、任意の2変数関数 ϕ 、 ψ に対して $f^{-1}(r_1/g, r_2) \neq \phi(m, g)$ 及び $f^{-1}(r_1/y_A, r_2) \neq \psi(m, y_A)$ となることを特徴とした請求項1記載の離散対数問題を用いた署名方式。

【請求項10】 写像 f_1 は、 $GF(p^2) \ni r_1, r_2, m, g, y_A$ に対し、 $r_2 = f_1(r_1, m)$ の逆像を $m = f_1^{-1}(r_1, r_2)$ で定義するとき、任意の2変数関数 ϕ 、 ψ に対して $f_1^{-1}(r_1/g, r_2) \neq \phi(m, g)$ 及び $f_1^{-1}(r_1/y_A, r_2) \neq \psi(m, y_A)$ となることを特徴とした請求項2記載の離散対数問題を用いた署名方式。

【請求項11】 写像 F は、 $E(GF(p)) \ni R_1, y_A$ 及び G 並びに $GF(p) \ni m$ 及び r_2 に対し、 $r_2 = f(R_1, m)$ の逆像を $m = f^{-1}(R_1, r_2)$ で定義するとき、任意の2変数関数 ϕ 、 ψ に対して $f^{-1}(R_1 - G, r_2) \neq \phi(m, G)$ 及び $f^{-1}(R_1 - y_A, r_2) \neq \psi(m, y_A)$ となることを特徴とした請求項3記載の離散対数問題を用いた署名方式。

【請求項12】 写像 F_1 は、 $E(GF(p^2)) \ni R_1, y_A$ 及び G 並びに $GF(p^2) \ni m$ 及び r_2 に対し、 $r_2 = f_1(R_1, m)$ の逆像を $m = f_1^{-1}(R_1, r_2)$ で定義するとき、任意の2変数関数 ϕ 、 ψ に対して

$f^{-1}(R_1 - G, r_2) \neq \psi(m, G)$

及び $f^{-1}(R_1 - Y_A, r_2) \neq \psi(m, Y_A)$

となることを特徴とした請求項4記載の離散対数問題を用いた署名方式。

【請求項13】 写像 f は、 $(r, y) \rightarrow r + y \text{ (GF}(p) \text{ 上の加算)}$ で定義されることを特徴とした請求項1記載のメッセージ復元型署名方式。

【請求項14】 写像 f は、 $(r, y) \rightarrow r + y \text{ (GF}(p^2) \text{ 上の加算)}$ で定義されることを特徴とした請求項2記載のメッセージ復元型署名方式。

【請求項15】 写像 f は、楕円曲線の x 座標関数を用いて、 $(R, y) \rightarrow x(R) + y \text{ (GF}(p) \text{ 上の加算)}$ で定義されることを特徴とした請求項3記載のメッセージ復元型署名方式。

【請求項16】 写像 f は、楕円曲線の x 座標関数を用いて、 $(R, y) \rightarrow x(R) + y \text{ (GF}(p^2) \text{ 上の加算)}$ で定義されることを特徴とした請求項4記載のメッセージ復元型署名方式。

【請求項17】 写像 π は、 $\{\alpha_1, \alpha_2, \dots, \alpha_z\}$ を $\text{GF}(p^2)$ の $\text{GF}(p)$ 上の基底とすると、 $\text{GF}(p^2)$ の元 $x = x_1\alpha_1 + \dots + x_z\alpha_z$ ($x_1, \dots, x_z \in \text{GF}(p)$) に対して、

$$\pi(x) = x_1 + x_2p + \dots + x_zp^{z-1}$$

で定義されることを特徴とした請求項2、同4、同6、同8、同10若しくは請求項12記載のメッセージ復元型署名方式。

【請求項18】 p を素数とし、有限体 $\text{GF}(p)$ の元を g とし、その位数を q とし、

$\text{GF}(p)$ 上定義される署名方式において、署名者 A の秘密鍵を x_A 、公開鍵を $y_A = g^{x_A}$ とし、署名したい文を $m \in \text{GF}(p)$ とするとき、 k を署名者が任意にとる乱数とし、 r_2 をコミットメント $r_1 = g^k$ と m により計算される $\text{GF}(p)$ の元とし、 $r_2' \equiv r_2 \pmod{q}$ とし、

ha, hb, hc を有限環 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、

$$ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$$

から s が計算できるように構成することを特徴としたメッセージ復元型署名方式。

【請求項19】 p を素数とし、 r を正整数とし、有限体 $\text{GF}(p^2)$ の元を s とし、その位数を q とし、

$\text{GF}(p^2)$ 上定義される署名方式において、署名者 A の秘密鍵を x_A 、公開鍵を $y_A = g^{x_A}$ とし、署名したい文を $m \in \text{GF}(p^2)$ とするとき、

k を署名者が任意にとる乱数とし、 r_2 をコミットメント $r_1 = g^k$ と m により計算される有限環 Z_{p^2} の元とし、 $r_2' \equiv r_2 \pmod{q}$ とし、

ha, hb, hc を有限環 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、

$$ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$$

$q)$

から s が計算できるように構成することを特徴としたメッセージ復元型署名方式。

【請求項20】 p を素数とし、有限体 $\text{GF}(p)$ 上定義された楕円曲線を E とし、

$E(\text{GF}(p))$ の元を G とし、その位数を q とし、

$E(\text{GF}(p))$ 上定義される署名方式において、署名したい文を $m \in \text{GF}(p)$ とするとき、

k を署名者が任意にとる乱数とし、 r_2 をコミットメント $R_1 = kG$ と m により計算される $\text{GF}(p)$ の元とし、 $r_2' \equiv r_2 \pmod{q}$ とし、

ha, hb, hc を有限環 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、

$$ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$$

から s が計算できるように構成することを特徴としたメッセージ復元型署名方式。

【請求項21】 p を素数とし、 r を正整数とし、有限体 $\text{GF}(p^2)$ 上定義された楕円曲線を E とし、

$E(\text{GF}(p^2))$ の元を G とし、その位数を q とし、

$E(\text{GF}(p^2))$ 上定義される署名方式において、署名したい文を $m \in \text{GF}(p^2)$ とするとき、

k を署名者が任意にとる乱数とし、 r_2 をコミットメント $R_1 = kG$ と m により計算される有限環 Z_{p^2} の元とし、 $r_2' \equiv r_2 \pmod{q}$ とし、

ha, hb, hc を有限環 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、

$$ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$$

から s が計算できるように構成することを特徴としたメッセージ復元型署名方式。

【請求項22】 写像 ha, hb, hc は、 r_2', s を Z_q の元とすると、別途予め固定された所定値を除く任意の Z_q の元 rr_2' 、 ss に対して、次の二つの条件

1. $ha(r_2', s, 1) = ha(rr_2', ss, 1)$, $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ のとき

$hb(r_2', s, 1) - ha(r_2', s, 1) \neq hb(rr_2', ss, 1)$

2. $ha(r_2', s, 1) = ha(rr_2', ss, 1)$, $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき

$hc(r_2', s, 1) - ha(r_2', s, 1) \neq hc(rr_2', ss, 1)$

を満足することを特徴とした請求項18、同19、同20若しくは請求項21記載の離散対数問題を用いた署名方式。

【請求項23】 写像 ha, hb, hc は、

$ha(r_2', s, 1) = 2r_2'$, $hc(r_2', s, 1) = s$ とし、

$hb(r_2', s, 1)$ は、

$r_2' = rr_2'$, $s = ss$ のとき、 $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ 、

$r_2' = rr_2'$, $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき、 $s = ss$ 、

$hb(0, 0, 1) \neq 0$ 、

を満たすことを特徴とした請求項22記載のメッセージ復元型署名方式。

【請求項24】 写像 ha, hb, hc は、

$ha(r_2', s, 1) = s$, $hc(r_2', s, 1) = r_2'$ とし、
 $hb(r_2', s, 1)$ は、
 $s = ss$, $r_2' = rr_2'$ のとき、 $hb(r_2', s, 1) = hb(rr_2', ss, 1)$

$s = ss$, $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき、 $r_2' = rr_2'$ 、
 $hb(0, 0, 1) \neq 0$

を満たすことを特徴とした請求項2記載のメッセージ復元型署名方式。

【請求項25】 写像 ha, hb, hc は、
 $ha(r_2', s, 1) = s$, $hb(r_2', s, 1) = r_2'$ とし、
 $hc(r_2', s, 1)$ は、
 $r_2' = rr_2'$, $s = ss$ のとき、 $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ 、
 $s = ss$, $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ のとき、 $r_2' = rr_2'$ 、
 $hc(0, 0, 1) \neq 0$

を満たすことを特徴とした請求項2記載のメッセージ復元型署名方式。

【請求項26】 写像 ha, hb, hc は、
 $ha(r_2', s, 1) = r_2'$, $hb(r_2', s, 1) = s$ とし、
 $hc(r_2', s, 1)$ は、
 $r_2' = rr_2'$, $s = ss$ のとき、 $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ 、
 $r_2' = rr_2'$, $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ のとき、 $s = ss$ 、
 $hc(0, 0, 1) \neq 0$

を満たすことを特徴とした請求項2記載のメッセージ復元型署名方式。

【請求項27】 写像 ha, hb, hc は、
 $hc(r_2', s, 1) = s$, $hb(r_2', s, 1) = r_2'$ とし、
 $ha(r_2', s, 1)$ は、
 $r_2' = rr_2'$, $ha(r_2', s, 1) = ha(rr_2', ss, 1)$ のとき、 $s = ss$ 、
 $s = ss$, $ha(r_2', s, 1) = ha(rr_2', ss, 1)$ のとき、 $r_2' = rr_2'$ 、
 $ha(0, 0, 1) \neq 0$

を満たすことを特徴とした請求項2記載のメッセージ復元型署名方式。

【請求項28】 写像 ha, hb, hc は、
 $hc(r_2', s, 1) = r_2'$, $hb(r_2', s, 1) = s$ とし、
 $ha(r_2', s, 1)$ は、
 $r_2' = rr_2'$, $ha(r_2', s, 1) = ha(rr_2', ss, 1)$ のとき、 $s = ss$ 、
 $s = ss$, $ha(r_2', s, 1) = ha(rr_2', ss, 1)$ のとき、 $r_2' = rr_2'$ 、
 $ha(0, 0, 1) \neq 0$

を満たすことを特徴とした請求項2記載のメッセージ復元型署名方式。

【請求項29】 写像 $hb(r_2', s, 1)$ は、
 $hb(r_2', s, 1) = r_2' + s + 1$
 で定義されることを特徴とした請求項23若しくは請求項24記載のメッセージ復元型署名方式。

【請求項30】 写像 $hb(r_2', s, 1)$ は、
 $hb(r_2', s, 1) = r_2' \times s + 1$
 で定義されることを特徴とした請求項23若しくは請求項24記載のメッセージ復元型署名方式。

【請求項31】 写像 $hc(r_2', s, 1)$ は、
 $hc(r_2', s, 1) = r_2' + s + 1$

で定義されることを特徴とした請求項25若しくは請求項26記載のメッセージ復元型署名方式。

【請求項32】 写像 $hc(r_2', s, 1)$ は、
 $hc(r_2', s, 1) = r_2' \times s + 1$

で定義されることを特徴とした請求項25若しくは請求項26記載のメッセージ復元型署名方式。

【請求項33】 写像 $ha(r_2', s, 1)$ は、 $ha(r_2', s, 1) = 0$ となる解 (r_2', s) がビットの多項式で定まる有限時間で確定できることを特徴とした請求項27若しくは請求項28記載のメッセージ復元型署名方式。

【請求項34】 乱数 k を、メッセージマスクで計算される r_2 と署名式で計算される s に対して、
 $ha(r_2', s, 1) \neq 0$

であるように取ってくることが特徴とした請求項33記載のメッセージ復元型署名方式。

【請求項35】 写像 $ha(r_2', s, 1)$ は、
 $ha(r_2', s, 1) = r_2' + s + 1$ であることを特徴とした請求項34記載のメッセージ復元型署名方式。

【請求項36】 写像 $ha(r_2', s, 1)$ は、
 $ha(r_2', s, 1) = r_2' \times s + 1$ であることを特徴とした請求項34記載のメッセージ復元型署名方式。

【請求項37】 p を素数とし、 q の $1/4$ 以上となる正整数とし、有限体 $GF(p)$ の位数が q となる元を g とし、

$GF(p)$ 上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、乱数 k を、コミットメント $r_1 = g^k$ と m により構成される $GF(p)$ の $元r_2$ が、

$0 < r_2 < q$ となるようにとり、
 上記範囲を限定された r_2 を署名式に用いることを特徴としたメッセージ復元型署名方式。

【請求項38】 p を素数とし、 r を正整数とし、 q を p と大きさがほぼ同じである、すなわち $p \sim q$ となる正整数とし、有限体 $GF(p^2)$ の位数が q となる元を g とし、

$GF(p^2)$ 上定義される署名方式において、署名したい文を $m \in GF(p^2)$ とするとき、乱数 k を、コミットメント $r_1 = g^k$ と m により構成される $Z_{p^2} = \{0, 1, \dots, p^2 - 1\}$ の $元r_2$ が、

$0 < r_2 < q$ となるようにとり、
 上記範囲を限定された r_2 を署名式に用いることを特徴としたメッセージ復元型署名方式。

【請求項39】 p を素数とし、有限体 $GF(p)$ 上定義された楕円曲線を E とし、
 $E(GF(p))$ の元を G とし、その位数を q とし、
 $E(GF(p))$ 上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、乱数 k を、コミットメント $r_1 = g^k$ と m により構成される $GF(p)$ の $元r_2$ が、

$0 < r_2 < q$ となるようにとり、
 上記範囲を限定された r_2 を署名式に用いることを特徴としたメッセージ復元型署名方式。

【請求項40】 p を素数とし、有限体 $GF(p)$ 上定義された楕円曲線を E とし、
 $E(GF(p))$ の元を G とし、その位数を q とし、
 $E(GF(p))$ 上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、乱数 k を、コミットメント $r_1 = g^k$ と m により構成される $GF(p)$ の $元r_2$ が、

$0 < r_2 < q$ となるようにとり、
 上記範囲を限定された r_2 を署名式に用いることを特徴としたメッセージ復元型署名方式。

【請求項40】 p を素数とし、 r を正整数とし、有限体 $GF(p^r)$ 上定義される楕円曲線を E とし、 $E(GF(p^r))$ の元を G とし、その位数を q とし、 $E(GF(p^r))$ 上定義される署名方式において、署名したい文を $m \in GF(p^r)$ とするとき、乱数 k を、コミットメント $r_1 = g^k$ と m により構成される $Z_{p^2} = \{0, 1, \dots, p^{r-1}\}$ の元 r_2 が、 $0 < r_2 < q$ となるようにとり、上記範囲を限定された r_2 を署名式に用いることを特徴としたメッセージ復元型署名方式。

【請求項41】 楕円曲線 E は、元の個数が p となる $GF(p)$ 上の楕円曲線を用いることを特徴とした請求項39記載の署名方式。

【請求項42】 署名したい文 m に対し、 m のハッシュ関数値 $hash(m)$ を m の代わりに用いることを特徴とした請求項1、同2、同3、同4、同18、同19、同20、同21、同37、同38、同39若しくは請求項40記載の署名方式。

【請求項43】 p を素数とし、有限体 $GF(p)$ の元を g とし、その位数を q とし、 $GF(p)$ 上定義される署名方式において、署名者 A の秘密鍵を x_A 、公開鍵を $y_A = g^{x_A}$ とし、署名したい文を $m \in GF(p)$ とするとき、 k を署名者が任意にとる乱数とし、コミットメント $r_1 = g^k$ とし、 $r_1' = r_1 \pmod{q}$ 、 $m' = m \pmod{q}$ とし、 ha, hb, hc を有限環 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、 $ha(r_1', s, m')k = hb(r_1', s, m') + hc(r_1', s, m')x_A \pmod{q}$ から s が計算できるように構成することを特徴とした署名方式。

【請求項44】 p を素数とし、 r を正整数とし、有限体 $GF(p^r)$ の元を g とし、その位数を q とし、 $GF(p^r)$ 上定義される署名方式において、署名者 A の秘密鍵を x_A 、公開鍵を $y_A = g^{x_A}$ とし、署名したい文を $m \in GF(p^r)$ とするとき、 k を署名者が任意にとる乱数とし、コミットメント $r_1 = g^k$ とし、 $GF(p^r)$ から有限環 Z_{p^2} への写像を π とするとき、 $r_1' = \pi(r_1) \pmod{q}$ 、 $m' = \pi(m) \pmod{q}$ とし、 ha, hb, hc を有限環 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、 $ha(r_1', s, m')k = hb(r_1', s, m') + hc(r_1', s, m')x_A \pmod{q}$ から s が計算できるように構成することを特徴とした署名方式。

【請求項45】 p を素数とし、有限体 $GF(p)$ 上定義された楕円曲線を E とし、 $E(GF(p))$ の元を G とし、その位数を q とし、

$E(GF(p))$ 上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、 k を署名者が任意にとる乱数とし、コミットメント $R_1 = g^k$ とし、 $E(GF(p))$ から $GF(p)$ への写像を ρ とするとき、 $r_1' = \rho(R_1) \pmod{q}$ 、 $m' = m \pmod{q}$ とし、 ha, hb, hc を有限環 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、 $ha(r_1', s, m')k = hb(r_1', s, m') + hc(r_1', s, m')x_A \pmod{q}$ から s が計算できるように構成することを特徴とした署名方式。

【請求項46】 p を素数とし、 r を正整数とし、有限体 $GF(p^r)$ 上定義された楕円曲線を E とし、 $E(GF(p^r))$ の元を G とし、その位数を q とし、 $E(GF(p^r))$ 上定義される署名方式において、署名したい文を $m \in GF(p^r)$ とするとき、 k を署名者が任意にとる乱数とし、コミットメント $R_1 = g^k$ とし、 $E(GF(p^r))$ から $GF(p^r)$ への写像を ρ とするとき、 $GF(p^r)$ から有限環 $Z_{p^2} = \{0, 1, \dots, p^{r-1}\}$ への写像を π とするとき、 $r_1' = \pi(\rho(R_1)) \pmod{q}$ 、 $m' = \pi(m) \pmod{q}$ とし、 ha, hb, hc を有限環 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、 $ha(r_1', s, m')k = hb(r_1', s, m') + hc(r_1', s, m')x_A \pmod{q}$ から s が計算できるように構成することを特徴とした署名方式。

【請求項47】 写像 ρ は、楕円曲線の x 座標若しくは y 座標関数を用いて、 $R \rightarrow x(R)$ 若しくは $R \rightarrow y(R)$ で定義されることを特徴とした請求項45若しくは請求項46記載のメッセージ復元型署名方式。

【請求項48】 写像 π は、 $\{\alpha_1, \alpha_2, \dots, \alpha_z\}$ を $GF(p^r)$ の $GF(p)$ 上の基底とすると、 $GF(p^r)$ の元 $x = x_1\alpha_1 + \dots + x_z\alpha_z$ ($x_1, \dots, x_z \in GF(p)$) に對して、 $\pi(x) = x_1 + x_2p + \dots + x_zp^{r-1}$ で定義されることを特徴とした請求項44及び請求項46記載のメッセージ復元型署名方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報の通信保持技術に関し、特に、離散対数問題を安全性の根拠として用いるデジタル署名技術に関する。

【0002】

【従来の技術】

（発明の技術的背景）本願発明に直接関係する技術は、我々では未だ必ずしも一般に周知とは言いがたいので、まず、間接的に関係する技術も含めて公開デジタル通信網を使用した暗号通信技術を広く一般的に説明する。

なお、この秘密通信方式等の一般技術については、わが国では、学術書としては池野信一、小山謙二著「現代暗号理論」電子通信学会発行 1986年、一般向けとしては、松、信吾「暗号の数理」講談社刊1980年に詳しい。

【0003】近年、一般に公開されたデジタル通信回線網を使用して相互に通信を行ったり、有料で放送番組を提供したりすることがさかんになってきている。ところで、一般に公開された通信回線網を使用する場合、第三者による盗聴や詐称、あるいは送信者による送信先の間違いを完全に防止することは困難である。このため、秘密通信方式並びに署名及び認証方式と呼ばれる通信方式が重要なものとなっている。ここに、秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行う方式である。また署名及び認証通信方式とは、通信相手に通信内容の正当性を示したり、本人であることを証明する通信方式である。さて、この秘密通信及び署名、認証通信の方式には、公開鍵暗号とよばれる数値を利用した方式がある。そして、この公開鍵暗号による方式は、NTT等の公開デジタル通信網により、国内外の多数の相手と通信を行う等のごく通信相手が多数、しかも通信者が相互に暗号技術について本来的に素人であるとき、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、現在では多数の通信相手と通信を行うのに不可欠な基盤技術とされている。

【0004】以下、この暗号通信技術の基本的原理と手順と特徴を2、3簡単に説明する。

(1) 有限体上の離散対数問題を使用した秘密通信方式。

なお、これはニールコブリッツ著「A Course in Number Theory and Cryptography」, Springer-Verlag, 1987)に詳しく述べられている。

(原理) p を素数、 g をその一の原始根、 u を任意の自然数、 a を g の u 乗の p を法とする剰余とする。すなわち、 $g^u \equiv a \pmod{p}$ とする。この場合、 g と p と u を与えられたときに a を求めるのは容易である。しかし、 p が 140 桁程度の素数となると、大型計算機の発達した今日でも、 g と p と a から u を求めるのは困難である。これは丁度、2つの素数 r と s があるとき r と s からその積を求めるのは容易であるが、 r と s が各 140 桁程度となれば、積は 280 桁となるため、これから素因数分解により r と s を求めるのは困難なことに似る。

(2) 楕円曲線上の離散対数問題を使用した秘密通信方式。

【0005】しかしながら、近年の大型計算機の発達を背景にして、数学の理論(類体論の高次相互律、分解法則等)を使用して、 g と p と a とから比較的少ない計算

量で u を求める方法が種々開発されつつある。その対策の一としては、素数 p を 140 桁程度のものでなく 200 桁等充分に大きいものとすることがあげられる。ただし、この場合には、桁数が大きいために、送受信に際して必要な計算の絶対量が多くなる等の不都合が生じる。

【0006】これらのため、楕円曲線を使用した秘密通信方式が開発された。

(原理) 次に $E\{GF(q)\}$ の性質、すなわち秘密通信の根拠の原理について説明する。 $E\{GF(q)\}$ の位数が大きな素数で割れる元 B をベースポイント、 d は任意の自然数とする。このとき、 B と d とから $d \cdot B$ を計算する (B を d 回加える) のは容易である。しかし、 $E\{GF(q)\}$ の与えられた元 Q と B に対して、 $Q = d \cdot B$

となる自然数 d が存在するならば d を求めよという問題は、計算機の発達した今日でも B や q 等が 30 桁程度の自然数となるならば困難である。なお、ここに B は、 p を法とする有限体 $GF(p)$ 上での g に相当する役を担うものである。

【0007】以上で、暗号通信の一般技術の概略説明は終了する。

(3) 署名、認証通信

次に、本願発明に関係する技術たる署名、認証通信について説明する。有限体上の離散対数問題におけるユーザ U とユーザ V の共有鍵 k_{uv} を使用しての秘密通信を例にとるならば、ユーザ U あるいはユーザ V にとって、一番最初に確かに相手にユーザ V あるいはユーザ U であることを認証すること、すなわち第三者による詐称を排除する必要がある。

【0008】この場合、ユーザ U とユーザ V とが面談、書留郵便等により直接確認する手段もあるが、国際間ではもとより国内の通信においても煩雑となる。この解決手段として、通信網による公開された数値情報を利用して署名、認証を行う技術が開発されている。以下この技術について、2、3紹介する。

(通信網提供者による署名認証) 最初、システム初期設定として、通信網提供者が、その秘密鍵 X と、端末の秘密鍵を生成するためのある秘密鍵生成関数 S を保有し、端末の公開鍵を生成するための所定の公開鍵生成関数 P と、所定の方向性関数 F と、秘密鍵 X を方向性関数 F に入力したときの出力値 $Y = F(X)$ とを端末情報実行センターの公開情報として公開デジタル通信網を使用する各ユーザに通知する。

【0009】次に、送信に際して、送信者の正当性の証明を欲するユーザ U が、その端末固有の識別情報 ID_U と、自分で作成した秘密鍵をもとに作成した公開値をセンターに通知し、その登録を請求する。なお、秘密鍵 x と公開値との間には、 $x = S(x, y, k, ID_U)$ の

関係がある。ここに、 $y = F(k)$ 、また k は乱数値である。

【0010】ユーザUからの請求を受けた通信網提供者が、ユーザUの公開鍵 y 、を他のユーザに公開する。すなわち、ユーザUは、検証用公開鍵として、その秘密鍵 x を前記一方向性関数 F に入力したときの出力値 $y_0 = F(x)$ を生成し、送信相手となるユーザVに対して、自分の公開情報として、その公開鍵 y と識別情報IDuと y_0 を、公開デジタル通信網を介して転送する。

【0011】ユーザVは、ユーザUからその端末公開情報の転送を受けると、ユーザUの公開鍵として、網提供者の公開情報Yと、ユーザUの公開鍵 y と、その識別情報IDuとを公開鍵生成関数Pに入力したときの出力値 $C = P(Y, y, IDu)$ を生成すること、生成されたユーザUの公開鍵Cと前記検証用公開鍵 y_0 を比較し、一致するか否かを確認する。一致したならば、確かに送信者はユーザUであると認める。

【0012】これにより、ユーザVは網提供者の発行した公開鍵Yを使用してユーザUから送信されてきた公開鍵を入手しえ、ひいては確かにユーザUから送られてきたものと認められる。以上の概略の手順、必要な構成を図2に示す。なお、認証は必ずしも通信網提供者とは限らないのも勿論である。

【0013】次に、具体的な関数式、関数値としての各鍵の値等としては、Yは、式 $Y = F(X) \equiv g^x \pmod{p}$ 等が用いられ、 K_u は乱数発生機により計算され、 Y_u は、式 $Y_u \equiv g^u \pmod{p}$ により計算され、 xu は、式 $xu \equiv S(X, y_u, k_u, IDu) \equiv X \times y_u + k_u \times IDu \pmod{\phi}$ 、(ここに、 ϕ は p のオイラー関数値)等により計算され、 P_u は、式 $P_u \equiv P(Y, y_u, IDu) \equiv (Y \wedge y_u) \times (y_u \wedge IDu) \pmod{p}$ 等により計算される。なおここに、オイラーの関数 ϕ とは、整数である変数の値より小さいかつその変数と互に素な整数の個数をいい、例えば $\phi(p) = p - 1$ 、 $\phi(10) = 2$ (注、1と5)、 $\phi(10) = 4$ (注、1、3、7、9)である。また、任意の互に素な2つの整数 u と v の間には、 $u \wedge v \pmod{p} - 1 \equiv 0 \pmod{p}$ という関係が常に成立する。例えば、 $3 \wedge 10 - 1 \equiv 3 - 1 \equiv 8 \equiv 0 \pmod{10}$ である。また、素数 p については、必ず $n^p - 1 \equiv 0 \pmod{p}$ となり、この対偶として、任意の整数 m について、何か1つの整数 n に対して $n^p - 1 \equiv 0 \pmod{p}$ が成立しないならば、 m は素数でないことがわかる。

(第3者による署名、認証) 次に、ユーザUとユーザVとの認証に第三のユーザWを介する方式もある。この場合には、ユーザUとユーザW、ユーザVとユーザWとは相互に認証が必要であるが、ユーザUとユーザVとの直接の認証は不要となる。そしてこれは、銀行(ユーザWに相当)を介しての金銭取引等で重要である。

【0014】なお、これら署名、認証の内容、方式については別途本願出願人が、特願平2-324479号「公開鍵生成方法及び装置」等にて開示し、また前掲の現代暗号理論にても種々記載されている周知技術であるため、これ以上の説明は省略する。

(4) メッセージ復元署名

次に、署名、認証についての技術の一として、本願発明に直接関係するメッセージ復元型署名について説明する。

【0015】1993年にNyberg-Rueppelにより離散対数問題に安全性の根拠をおくメッセージ復元型署名が発表された。以下に離散対数問題を用いたメッセージ復元型署名のひとつについて述べる。これについて詳しくは、Nyberg and Rueppel, "A new signature scheme based on the DSA giving message recovery", 1st ACM Conf. on Comp. and Comm. Security, 1993 を参照された。

(メッセージ復元型署名の従来例) 図3は、従来技術としての、上記Nyberg-Rueppel方式におけるメッセージ復元型署名の手順及び構成を示すものである。

【0016】以下、本図を参照しながら従来例の手順を説明する。

(1) センターによる初期設定

p を素数、 $G(p, p)$ の元 g としその位数を q とする。センターは、システムパラメータとして p, q, g を全ユーザ、すなわち公開デジタル通信網に接続された全端末に公開する。

(2) ユーザAによる秘密鍵の生成と公開鍵の登録要求の発生。

【0017】署名通信を希望するユーザAが、その端末情報とを作成し、これを使用しての秘密鍵と対応する公開鍵も作成し、公開鍵の登録をセンターに要求する。このためユーザAは、乱数 x_A を発生させ、これを自分の秘密鍵 x_A とし、対応する公開鍵を $y_A \equiv g^{x_A} \pmod{p}$ により求める。更にセンターを経由して、全ユーザにユーザAの公開鍵 y_A を公開する。

(3) ユーザAによる署名の生成及び送信。

【0018】ユーザBに署名、認証通信の発信を行うユーザAは、以下の処理を行う。

1. 乱数 k を生成させる。

$$r_1 \equiv g^k \pmod{p}$$

$$r_2 \equiv m / r_1 \pmod{p} \cdots (a)$$

$$r_2' \equiv -r_2 \pmod{q}$$

$$s \equiv k - r_2' \times x_A \pmod{q} \cdots (b)$$

【0019】3. ユーザAは (r_2, s) を、ユーザBに送信する。

(4) ユーザBによる受信したメッセージの復元
ユーザBは、以下の式を計算することにより、メッセー

j_m を復元する。

$$1. g^{s \cdot y_A} \cdot r_2^{z^2} \cdot r_2 \equiv m \pmod{p}$$

ここで、上記 r_1 はコミットメントと呼ばれ、(a)はメッセージマスク式、(b)は署名式と呼ばれる。

【0020】上記従来例は、従来不可能であった離散対数問題に基づくメッセージ復元型署名を可能にする。また署名式(b)は以下のように6(=3!)種類の式に一般化される。

$$ak = b + cx_A \pmod{q}, (a, b, c) = (1, r_2', s) \text{の置換} \cdots (b')$$

【0021】

【発明が解決しようとする課題】しかしながら、この従来例のメッセージ復元型署名に対しては、式が(a)と(b)が簡単のため変形が容易であり、例えば y_A 及ぶ g のべき乗並びに m についての掛け算の式が、3変数より2変数の式に置換しえる等のため近年幾つかの攻撃 recovery-equation attack using g and y_A , signature-equation attack using g and y_A , and homomorphism attack (各「 g と y_A を使用した再生攻撃」、「 g と y_A を使用した署名攻撃」及び「準同型攻撃(選択平文攻撃)」が発表された。これについて詳しくは、宮地 充子、「メッセージ復元型署名の弱点1」、電子情報通信学会、情報セキュリティ研究会、1995、7月及びNyberg and Rueppel, "A new signature scheme based on the DSA giving message recovery", 1st ACM Conf. on Comp. and Comm. Security, 1993及びNyberg and Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem", Advances in cryptology-Proceedings of Eurocrypt'94, Lecture Notes in Computer Science, 950(1995), Springer-Verlag, 182-193を参照されたい。なお、参考までにその攻撃の1つを図4に示す。

【0022】これらに加えて、次に述べる冗長性を利用した攻撃(redundancy attack)が存在する。署名通信等では、解読の困難性からは p 、 q は大きい程好ましいが、必要な演算が少なくて済む等の面からは小さい方が好ましい。このかねあひから実際的には p は512ビット、1024ビット程度の素数を使用されるが、 q は160ビット程度の数を使用される。この場合、上記 $r_2' \equiv r_2 \pmod{q}$ の式では、 p 以下で $r_2' \equiv r_2$ 以外にこの式を満たす数 r_2 が存在しうる。本読解はこれを利用したものである。

【0023】今、偽造者が一つの署名(r_2, s)を手に入れたとき、容易にこの署名文 m が復元できるが、このとき $rr_2 = r_2' + tq \pmod{p}$ (ここに、 r_2 とは r_2 の偽を意味する。)

$$mm = rr_2 \cdot (m/r_2)$$

(ここに、 mm とは、 m の偽を意味する)を計算し、第三者に(rr_2, s)を送信する。これを受け取った第三者は、Aの公開鍵を用いて従来例に示した復元

方法で mm を復元し、Aから送られたと思ってしまう。この結果、偽造者はAになりますことができる。

【0024】参考までに、この攻撃の概要を図5に示す。なお、本図の「ナルゲル」は偽造者が署名を生成することを意味する。これら6つの攻撃により、上記従来例のメッセージ復元型署名方式は、署名式の形によらず、ある文の署名の偽造が一部の文と署名のペアを得るだけで可能になり、安全な式とはいえなくなった。

【0025】そして、これらのことは、楕円曲線を使用した場合にもあてはまる。以上説明してきたように最近になってメッセージ復元型署名は、その解読方法が考案され、このためこの署名は安全でないことがわかった。この解読方法は従来の署名(メッセージを復元できない署名)には適応できないことがわかっていて、しかし、メッセージ復元性は有用な性質であり、この性質を保持しつつ解読が回避できることが望ましいといって、あまり複雑な署名式、メッセージマスク式を採用したりするのは、必要な計算量の減少を図るという面から好ましくない。

【0026】本発明は、この従来例における問題点を鑑みてなされたもので、メッセージ復元性を保ちながら、提案された各種の解読に対して強い、しかも必要な計算量の少ないメッセージ復元型署名方式を提供することを目的とする。

【0027】

【課題を解決するための手段】本発明における署名方式は、 p を素数とし、有限体 $GF(p)$ の元を g とし、その位数を q とし、 $GF(p)$ 上定義される署名方式において、署名者Aの秘密鍵を x_A 、公開鍵を $y_A = g^{x_A}$ とし、署名したい文を $m \in GF(p)$ とすると、 k を署名者が任意にとる乱数とし、コミットメント $r_1 = g^k$ とし、 $r_1' \equiv r_1 \pmod{q}$ 、 $m' \equiv m \pmod{q}$ とし、 ha, hb, hc を有限環 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、 $ha(r_1', s, m')k \equiv hb(r_1', s, m') + hc(r_1', s, m')x_A \pmod{q}$ から s が計算できるように構成されている。これにより、各種の攻撃を回避する。

【0028】また、本発明におけるメッセージ復元を可能にするメッセージマスク式を使用したメッセージ復元型署名方式は、メッセージマスク式として、 p を素数とし、有限体 $GF(p)$ の元を g とし、その位数を q とし、 $GF(p)$ 上定義される署名方式において、署名したい文を $m \in GF(p)$ とすると、 k を署名者が任意にとる乱数とし、 $r_1 \equiv g^k \pmod{p}$ を署名生成処理におけるコミットメントとし、 $GF(p) \times GF(p)$ から $GF(p)$ への写像を f とすると、 r_1 と m を f により変換した $f(r_1, m)$ を用いる。これにより、各種の攻撃を回避する。

【0029】また、本発明における署名方式、メッセージ復元型署名方式は、 $E \cdot G(p^2)$ 、 $E \cdot GF(p)$ 、 $E \cdot GF(p^2)$ 上でもなされる。

【0030】

【発明の実施の形態】従来技術で記載した目的を達成するため、請求項1の発明では、特にGF(p) 上のメッセージ復元型署名において、p を素数とし、有限体GF(p) の元をg とし、その位数をq とし、GF(p) 上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、k を署名者が任意にとる乱数とし、 $r_1 = g^k$ を署名生成処理におけるコミットメントとし、GF(p) \times GF(p) からGF(p) への写像をf とするとき、 r_1 と m を f により変換した $f(r_1, m)$ を用いて署名生成処理におけるメッセージ復元を可能にすることを特徴としている。

【0031】請求項2の発明では、特にGF(p²) 上のメッセージ復元型署名において、p を素数とし、r を正整数とし、有限体GF(p²) の元をg とし、その位数をq とし、GF(p²) 上定義される署名方式において、署名したい文を $m \in GF(p^2)$ とするとき、k を署名者が任意にとる乱数とし、 $r_1 = g^k$ をコミットメントとし、GF(p²) \times GF(p²) からGF(p²) への写像をf₁ とし、GF(p²) から有限環 $Z_{p^2} = \{0, 1, \dots, p^2-1\}$ への写像を π とするとき、 r_1 と m を f₁ により変換し、この値を更に π を用いて変換した $\pi(f_1(r_1, m))$ を用いて署名生成処理におけるメッセージ復元を可能にすることを特徴としている。

【0032】請求項3の発明では、特にGF(p) 上のメッセージ復元型署名において、p を素数とし、有限体GF(p) 上定義された楕円曲線をE とし、E(GF(p))の元をG とし、その位数をq とし、E(GF(p))上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、k を署名者が任意にとる乱数とし、 $R_1 = kG = (r_x, r_y)$ をコミットメントとし、E(GF(p)) \times GF(p) からGF(p) への写像をF とするとき、 R_1 と m を f により変換した $f(R_1, m)$ を用いて署名生成処理におけるメッセージ復元を可能にすることを特徴としている。

【0033】請求項4の発明では、特にE(GF(p²)) 上のメッセージ復元型署名において、p を素数とし、r を正整数とし、有限体GF(p²) 上定義された楕円曲線をE とし、E(GF(p²))の元をG とし、その位数をq とし、E(GF(p²)) 上定義される署名方式において、署名したい文を $m \in GF(p^2)$ とするとき、k を署名者が任意にとる乱数とし、 $R_1 = kG = (r_x, r_y)$ をコミットメントとし、E(GF(p²)) \times GF(p²) からGF(p²) への写像をF₁ とし、GF(p²) から有限環 Z_{p^2} への写像を π とするとき、 R_1 と m を F₁ により変換し、この値を更に π を用いて変換した $\pi(F_1(R_1, m))$ を用いて署名生成処理におけるメッセージ復元を可能にすることを特徴としている。

【0034】請求項5の発明では、特にメッセージ復元型署名上のrecovery-equation 攻撃を回避するため、写像F は、GF(p) \ni g, y_A 及び m 並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$ 及び e_A に対し、 $f(g^t y_A^j, m)$ 及び $f(g^t y_A^j, m)$ において、3変数t, j, e_A が2個の代数式で非置換である(置き換えられない)ことを特徴としている。

【0035】請求項6の発明では、特にメッセージ復元型署名上のrecovery-equation 攻撃を回避するため、写像F は、GF(p²) \ni g, y_A 及び m 並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$ 及び e_A に対し、 $f_1(g^t y_A^j, m)$ 及び $f_1(g^t y_A^j, m)$ において、3変数t, j, e_A が2個の代数式で非置換である(置き換えられない)ことを特徴としている。

【0036】請求項7の発明では、特にメッセージ復元型署名上のrecovery-equation 攻撃を回避するため、写像F は、E(GF(p)) \ni G 及びY_A, GF(p) \ni m 並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$ 及び e_A に対し、 $f(tG + jY_A, m)$ \times $\times(e_A)$ 及び $f(tG + jY_A, m)$ \times $\times(e_A)$ において、3変数t, j, e_A が2個の代数式で非置換(置き換えられない)ことを特徴としている。

【0037】請求項8の発明では、特にメッセージ復元型署名上のrecovery-equation 攻撃を回避するため、写像F₁ は、E(GF(p²)) \ni G 及びY_A, GF(p²) \ni m 並びに $Z_{q^2} = \{0, 1, \dots, q^2-1\} \ni t, j$ 及び e_A に対し、 $f(tG + jY_A, m)$ \times $\times(e_A)$ 及び $f(tG + jY_A, m)$ \times $\times(e_A)$ において、3変数t, j, e_A が2個の代数式で非置換である(置き換えられない)ことを特徴としている。

【0038】請求項9の発明では、特にメッセージ復元型署名上のhomomorphism攻撃を回避するため、写像F は、GF(p) \ni r₁, r₂, m, g 及びy_A に対し、 $r_2 = f(r_1, m)$ の逆像を $m = f^{-1}(r_1, r_2)$ で定義するとき、任意の2変数関数 ψ に対して $f^{-1}(r_1/s, r_2) \neq \psi(m, y_A)$ 及び $f^{-1}(r_1/y_A, r_2) \neq \psi(m, y_A)$ となることを特徴としている。

【0039】請求項10の発明では、特にメッセージ復元型署名上のhomomorphism攻撃を回避するため、写像F₁ は、GF(p²) \ni r₁, r₂, m, g 及びy_A に対し、 $r_2 = f_1(r_1, m)$ の逆像を $m = f_1^{-1}(r_1, r_2)$ で定義するとき、任意の2変数関数 ψ に対して $f_1^{-1}(r_1/s, r_2) \neq \psi(m, y_A)$ 及び $f_1^{-1}(r_1/y_A, r_2) \neq \psi(m, y_A)$ となることを特徴としている。

【0040】請求項11の発明では、特にメッセージ復元型署名上のhomomorphism攻撃を回避するため、写像F は、E(GF(p)) \ni R₁, Y_A 及びG 並びにGF(p) \ni m 及びr₂ に対し、 $r_2 = f(R_1, m)$ の逆像を $m = f^{-1}(R_1, r_2)$ で定義するとき、任意の2変数関数 ψ に対して $f^{-1}(R_1 - G, r_2) \neq \psi(m, G)$ 及び $f^{-1}(R_1 - Y_A, r_2) \neq \psi(m, Y_A)$ となることを特徴としている。

【0041】請求項12の発明では、特にメッセージ復元型署名上のhomomorphism攻撃を回避するため、写像F₁ は、E(GF(p²)) \ni R₁, Y_A 及びG 並びにGF(p²) \ni m 及びr₂ に対し、 $r_2 = f_1(R_1, m)$ の逆像を $m = f_1^{-1}(R_1, r_2)$ で定義するとき、任意の2変数関数 ψ に対して $f_1^{-1}(R_1 - G, r_2) \neq \psi(m, G)$ 及び $f_1^{-1}(R_1 - Y_A, r_2) \neq \psi(m, Y_A)$ となることを特徴としている。

【0042】請求項13の発明では、特にメッセージ復

元型署名の上のrecovery-equation, homomorphism攻撃を回避するため、写像 f は、 $(r, y) \mapsto r + y \cdot \text{GF}(p)$ 上の加算)で定義されることを特徴としている。請求項14の発明では、特にメッセージ復元型署名の上のrecovery-equation, homomorphism攻撃を回避するため、写像 f は、 $(r, y) \mapsto r + y \cdot \text{GF}(p^2)$ 上の加算)で定義されることを特徴としている。

【0043】請求項15の発明では、特にメッセージ復元型署名の上のrecovery-equation, homomorphism攻撃を回避するため、写像 f は、楕円曲線の x 座標関数を用いて、 $(R, y) \mapsto x(R) + y \cdot \text{GF}(p)$ 上の加算)で定義されることを特徴としている。請求項16の発明では、特にメッセージ復元型署名の上のrecovery-equation, homomorphism攻撃を回避するため、写像 f は、楕円曲線の x 座標関数を用いて、 $(R, y) \mapsto x(R) + y \cdot \text{GF}(p^2)$ 上の加算)で定義されることを特徴としている。

【0044】請求項17の発明では、特にメッセージ復元型署名の上のrecovery-equation, homomorphism攻撃を回避するため、写像 π は、 $\{\alpha_1, \alpha_2, \dots, \alpha_r\}$ を $\text{GF}(p^r)$ の $\text{GF}(p)$ 上の基底とすると、 $\text{GF}(p^r)$ の元 $x = x_1\alpha_1 + \dots + x_r\alpha_r$ ($x_1, \dots, x_r \in \text{GF}(p)$)に対して、 $\pi(x) = x_1x_2p + \dots + x_r p^{r-1}$ で定義されることを特徴としている。

【0045】請求項18の発明では、 $\text{GF}(p)$ 上のメッセージ復元型署名の上の攻撃を回避するため、 p を素数とし、有限体 $\text{GF}(p)$ の元 g とし、その位数を q とし、 $\text{GF}(p)$ 上定義される署名方式において、署名者 A の秘密鍵を x_A 、公開鍵を $y_A = g^{x_A}$ とし、署名したい文を $m \in \text{GF}(p)$ とすると、 k を署名者が任意にとる乱数とし、 r_2 をコミットメント $r_1 = g^k$ と m により計算される $\text{GF}(p)$ の元とし、 $r_2' \equiv r_2 \pmod{q}$ とし、 ha, hb, hc を有限環 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、 $ha(r_2', s, 1)k \equiv hb(r_2', s, 1)k + hc(r_2', s, 1) \pmod{q}$ から s が計算できるように構成することを特徴としている。

【0046】請求項19の発明では、特に $\text{GF}(p^2)$ 上のメッセージ復元型署名の上の攻撃を回避するため、 p を素数とし、 r を正整数とし、有限体 $\text{GF}(p^2)$ の元 g とし、その位数を q とし、 $\text{GF}(p^2)$ 上定義される署名方式において、署名者 A の秘密鍵を x_A 、公開鍵を $y_A = g^{x_A}$ とし、署名したい文を $m \in \text{GF}(p^2)$ とすると、 k を署名者が任意にとる乱数とし、 r_2 をコミットメント $r_1 = g^k$ と m により計算される有限環 Z_{p^2} の元とし、 $r_2' \equiv r_2 \pmod{q}$ とし、 ha, hb, hc を有限環 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、 $ha(r_2', s, 1)k \equiv hb(r_2', s, 1)k + hc(r_2', s, 1) \pmod{q}$ から s が計算できるように構成することを特徴としている。

【0047】請求項20の発明では、特に $E(\text{GF}(p))$ 上のメッセージ復元型署名の上の攻撃を回避するため、 p を素数とし、有限体 $\text{GF}(p)$ 上定義された楕円曲線を E と

し、 $E(\text{GF}(p))$ の元 g とし、その位数を q とし、 $E(\text{GF}(p))$ 上定義される署名方式において、署名したい文を $m \in \text{GF}(p)$ とすると、 k を署名者が任意にとる乱数とし、 r_2 をコミットメント $r_1 = g^k$ と m により計算される $\text{GF}(p)$ の元とし、 $r_2' \equiv r_2 \pmod{q}$ とし、 ha, hb, hc を有限環 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、 $ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1) \pmod{q}$ から s が計算できるように構成することを特徴としている。

【0048】請求項21の発明では、特に $E(\text{GF}(p^2))$ 上のメッセージ復元型署名の上の攻撃を回避するため、 p を素数とし、 r を正整数とし、有限体 $\text{GF}(p^2)$ 上定義された楕円曲線を E とし、 $E(\text{GF}(p^2))$ の元 g とし、その位数を q とし、 $E(\text{GF}(p^2))$ 上定義される署名方式において、署名したい文を $m \in \text{GF}(p^2)$ とすると、 k を署名者が任意にとる乱数とし、 r_2 をコミットメント $r_1 = g^k$ と m により計算される有限環 Z_{p^2} の元とし、 $r_2' \equiv r_2 \pmod{q}$ とし、 ha, hb, hc を有限環 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、 $ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1) \pmod{q}$ から s が計算できるように構成することを特徴としている。

【0049】請求項22の発明では、特にメッセージ復元型署名の上のsignature-equation攻撃を回避するため、写像 ha, hb, hc は、 $r_2' \cdot s$ を Z_q の元とすると、予め固定された少数値を除く任意の Z_q の元 rr_2' 、 ss に対して、次の二つの条件1. $ha(r_2', s, 1) = ha(rr_2', ss, 1)$ 、 $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ のとき $hb(r_2', s, 1) = ha(r_2', s, 1) \neq hb(rr_2', ss, 1)$ 2. $ha(r_2', s, 1) = ha(rr_2', ss, 1)$ 、 $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき $hc(r_2', s, 1) = ha(r_2', s, 1) \neq hc(rr_2', ss, 1)$ を満足することを特徴としている。

【0050】請求項23の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 ha, hb, hc は、 $ha(r_2', s, 1) = r_2'$ 、 $hc(r_2', s, 1) = s$ とし、 $hb(r_2', s, 1)$ は、 $r_2' \cdot r_2'$ 、 $s = ss$ のとき、 $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ 、 $r_2' \cdot r_2'$ 、 $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき、 $s = ss$ 、 $hb(0, 0, 1) \neq 0$ を満たすことを特徴としている。

【0051】請求項24の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 ha, hb, hc は、 $ha(r_2', s, 1) = s$ 、 $hc(r_2', s, 1) = r_2'$ とし、 $hb(r_2', s, 1)$ は、 $s = ss$ 、 $r_2' = r_2'$ のとき、 $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ 、 $s = ss$ 、 $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき、 $r_2' = r_2'$ 、 $hb(0, 0, 1) \neq 0$ を満たすことを特徴としている。

【0052】請求項25の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 ha, hb, hc は、 $ha(r_2', s, 1) = s$ 、 $hb(r_2', s, 1) = r_2'$ とし、 $hc(r_2', s, 1)$ は、 $r_2' \cdot r_2'$ 、 $s = ss$ のとき、 $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ 、 $s = ss$ 、 $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ のとき、 $r_2' = r_2'$ 、 $hc(0, 0, 1) \neq 0$ を満たすことを特徴としている。

$r_2', ss, 1)$ のとき、 $r_2' = rr_2' \cdot hc(0, 0, 1) \neq 0$ を満たすことを特徴としている。

【0053】請求項26の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 ha, hb, hc は、 $ha(r_2', s, 1) = r_2'$ 、 $hb(r_2', s, 1) = s$ とし、 $hc(r_2', s, 1)$ は、 $r_2' = rr_2'$ 、 $s = ss$ のとき、 $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ 、 $r_2' = rr_2'$ 、 $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ のとき、 $s = ss$ 、 $hc(0, 0, 1) \neq 0$ を満たすことを特徴としている。

【0054】請求項27の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 ha, hb, hc は、 $hc(r_2', s, 1) = s$ 、 $hb(r_2', s, 1) = r_2'$ とし、 $ha(r_2', s, 1)$ は、 $r_2' = rr_2'$ 、 $ha(r_2', s, 1) = ha(rr_2', ss, 1)$ のとき、 $s = ss$ 、 $ha(r_2', s, 1) = ha(r_2', ss, 1)$ のとき、 $r_2' = rr_2'$ 、 $ha(0, 0, 1) \neq 0$ を満たすことを特徴としている。

【0055】請求項28の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 ha, hb, hc は、 $hc(r_2', s, 1) = r_2'$ 、 $hb(r_2', s, 1) = s$ とし、 $ha(r_2', s, 1)$ は、 $r_2' = rr_2'$ 、 $ha(r_2', s, 1) = ha(rr_2', ss, 1)$ のとき、 $s = ss$ 、 $ha(r_2', s, 1) = ha(r_2', ss, 1)$ のとき、 $r_2' = rr_2'$ 、 $ha(0, 0, 1) \neq 0$ を満たすことを特徴としている。

【0056】請求項29の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 $hb(r_2', s, 1)$ は、 $hb(r_2', s, 1) = r_2' + s + 1$ で定義されることを特徴としている。請求項30の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 $hb(r_2', s, 1)$ は、 $hb(r_2', s, 1) = r_2' \times s + 1$ で定義されることを特徴としている。

【0057】請求項31の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 $hc(r_2', s, 1)$ は、 $hc(r_2', s, 1) = r_2' + s + 1$ で定義されることを特徴としている。請求項32の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 $hc(r_2', s, 1)$ は、 $hc(r_2', s, 1) = r_2' \times s + 1$ で定義されることを特徴としている。

【0058】請求項33の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 $ha(r_2', s, 1)$ は、 $ha(r_2', s, 1) = 0$ となる解 (r_2', s) が有限時間（ビットデータの多項式、すなわち非指数時間）で確定できることを特徴としている。請求項34の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、乱数 k を、メッセージマスキングで計算される r_2 と署名式で計算される s に対して、 $ha(r_2', s, 1) \neq 0$ であるように取ってくることを特徴としている。

【0059】請求項35の発明では、特にメッセージ復

元型署名の上のsignature-equation、比例攻撃を回避するため、写像 $ha(r_2', s, 1)$ は、 $ha(r_2', s, 1) = r_2' + s + 1$ であることを特徴としている。請求項36の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 $ha(r_2', s, 1)$ は、 $ha(r_2', s, 1) = r_2' \times s + 1$ であることを特徴としている。

【0060】請求項37の発明では、特にGF(p)上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、qを $(P/4) < q$ となる正整数とし、有限体GF(p)の位数がqとなる元をgとし、GF(p)上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、乱数kを、コミットメント $r_1 = g^k$ とmにより構成されるGF(p)の元 r_2 が、 $0 < r_2 < q$ となるようにとり、上記範囲を限定された r_2 を署名式に用いることを特徴としている。

【0061】請求項38の発明では、特にGF(p²)上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、rを正整数とし、qを $(P/4) < q$ となる正整数とし、有限体GF(p²)の位数がqとなる元をgとし、GF(p²)上定義される署名方式において、署名したい文を $m \in GF(p^2)$ とするとき、乱数kを、コミットメント $r_1 = g^k$ とmにより構成される $Z_{p^2} = \{0, 1, \dots, p^2 - 1\}$ の元 r_2 が、 $0 < r_2 < q$ となるようにとり、上記範囲を限定された r_2 を署名式に用いることを特徴としている。

【0062】請求項39の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、有限体GF(p)上定義された楕円曲線をEとし、E(GF(p))の元をGとし、その位数をqとし、E(GF(p))上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、乱数kを、コミットメント $r_1 = g^k$ とmにより構成されるGF(p)の元 r_2 が、 $0 < r_2 < q$ となるようにとり、上記範囲を限定された r_2 を署名式に用いることを特徴としている。

【0063】請求項40の発明では、特にGF(p²)上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、rを正整数とし、有限体GF(p²)上定義された楕円曲線をEとし、E(GF(p²))の元をGとし、その位数をqとし、E(GF(p²))上定義される署名方式において、署名したい文を $m \in GF(p^2)$ とするとき、乱数kを、コミットメント $r_1 = g^k$ とmにより構成される $Z_{p^2} = \{0, 1, \dots, p^2 - 1\}$ の元 r_2 が、 $0 < r_2 < q$ となるようにとり、上記範囲を限定された r_2 を署名式に用いることを特徴としている。

【0064】請求項41の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、楕円曲線Eは、元の位数がqとなるGF(p)上の楕円曲線を用いることを特徴としている。請求項42の発明では、特にメッセージ復元型署名の上の攻撃を回避するため、署名したい文mに対し、mのハッシュ関数値hash(m)をm

の代わりに用いることを特徴としている。請求項43の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、有限体GF(p)の元をgとし、その位数をqとし、E(GF(p))上定義される署名方式において、署名者Aの秘密鍵を x_A 、公開鍵を $y_A = g^{x_A}$ とし、署名したい文を $m \in GF(p)$ とすると、 k を署名者が任意にとる乱数とし、コミットメント $r_1 = g^k$ とし、 $r_1^{-1} = r_1^{-1} \pmod{q}$ 、 $m' = m \pmod{q}$ とし、 h_A, h_B, h_C を有限域 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、 $h_A(r_1^{-1}, s, m')k \equiv h_B(r_1^{-1}, s, m') + h_C(r_1^{-1}, s, m')x_A \pmod{q}$ からsが計算できるよ

うに構成することを特徴としている。
【0065】請求項44の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、rを正整数とし、有限体GF(p^r)の元をgとし、その位数をqとし、GF(p^r)上定義される署名方式において、署名者Aの秘密鍵を x_A 、公開鍵を $y_A = g^{x_A}$ とし、署名したい文を $m \in GF(p^r)$ とすると、kを署名者が任意にとる乱数とし、コミットメント $r_1 = g^k$ とし、GF(p^r)から有限域 Z_{p^r} への写像を π とすると、 $r_1^{-1} \equiv \pi(r_1^{-1}) \pmod{q}$ 、 $m' \equiv \pi(m) \pmod{q}$ とし、 h_A, h_B, h_C を有限域 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、 $h_A(r_1^{-1}, s, m')k \equiv h_B(r_1^{-1}, s, m') + h_C(r_1^{-1}, s, m')x_A \pmod{q}$ からsが計算できるように構成することを特徴としている。

【0066】請求項45では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、有限体GF(p)上定義された楕円曲線をEとし、E(GF(p))の元をGとし、その位数をqとし、E(GF(p))上定義される署名方式において、署名したい文を $m \in GF(p)$ とすると、kを署名者が任意にとる乱数とし、コミットメント $R_1 = kg$ とし、E(GF(p))からGF(p)への写像を ρ とすると、 $r_1^{-1} = \rho(R_1^{-1}) \pmod{q}$ 、 $m' = m \pmod{q}$ とし、 h_A, h_B, h_C を有限域 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、 $h_A(r_1^{-1}, s, m')k \equiv h_B(r_1^{-1}, s, m') + h_C(r_1^{-1}, s, m')x_A \pmod{q}$ からsが計算できるように構成することを特徴としている。

【0067】請求項46の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、rを正整数とし、有限体GF(p^r)上定義された楕円曲線をEとし、E(GF(p^r))の元をGとし、その位数をqとし、E(GF(p^r))上定義される署名方式において、署名したい文を $m \in GF(p^r)$ とすると、kを署名者が任意にとる乱数とし、コミットメント $R_1 = kg$ とし、E(GF(p^r))からGF(p^r)への写像を ρ とすると、 $r_1^{-1} = \rho(R_1^{-1}) \pmod{q}$ 、 $m' = \pi(m) \pmod{q}$ とし、 h_A, h_B, h_C を有限域 $Z_q \times Z_q \times Z_q$ から Z_q への写像とすると、署名式を、 $h_A(r_1^{-1}, s, m')k \equiv h_B(r_1^{-1}, s, m') + h_C(r_1^{-1}, s, m')x_A \pmod{q}$ からs

が計算できるように構成することを特徴としている。

【0068】請求項47の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、写像 ρ は、楕円曲線のx座標若しくはy座標関数を用いて、 $R \rightarrow x(R)$ 若しくは $R \rightarrow y(R)$ で定義されることを特徴としている。請求項48の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、写像 π は、 $\{\alpha_1, \alpha_2, \dots, \alpha_x\}$ をGF(p^r)のGF(p)上の基底とすると、GF(p^r)の元 $x = x_1\alpha_1 + \dots + x_x\alpha_x$ ($x_1, \dots, x_x \in GF(p)$)に対して、 $\pi(x) = x_1\alpha_1 + \dots + x_x\alpha_x$ で定義されることを特徴としている。

【0069】

【実施例】

(第1実施例)以下、本発明を実施例に基づいて説明する。以下、本発明の第1実施例を、図を参照しつつ説明する。まず、公開デジタル通信網全体の構成について説明する。

【0070】図6は、本発明が実施される公開デジタル通信網全体の構成図である。本図において、1は通信網提供者である。2は、公開デジタル通信回線である。2はデジタル通信回線である。3〜6は、公開デジタル通信回線2に接続されたユーザ端末(以下、単に「ユーザ」と言う)A、ユーザB、…、ユーザU、ユーザVである。本図に示すように、通信網提供者は、システムパラメータとして、2進数512ビットで表される素数p、

$$g^q \equiv 1 \pmod{p}$$

となる最小の整数(位数)qが256ビットの整数qである整数g、GF(p)上で $f(r_1, m) \equiv r_1 + m \pmod{p}$ そしてその逆写像 f^{-1} が $f^{-1}(r_1, f(r_1, m)) \equiv m \pmod{p}$ を充たすメッセージマスキング $f, Z \times G \times Z \times G$ からZgへの写像で、 $h_A(r_2', s, 1) = s, h_B(r_2', s, 1) \equiv r_2' + s + 1 \pmod{q}, h_C(r_2', s, 1) \equiv r_2'$ を充たす関数 h_A, h_B, h_C をシステムパラメータと各ユーザに公開している。

【0071】次に、図6に示す通信網提供者1とユーザ3〜6の構成について説明する。図7は、通信網提供者1により提供されたICカードやユーザ自身が作成したパソコン用プログラムの要部の構成図である。本図において、11は秘密鍵作成要求受付部である。12は、秘密鍵発生部である。13は、公開鍵作成部である。14は、公開鍵公開部である。15は、秘密鍵通知形態作成部である。16は、秘密鍵通知部である。

【0072】131は公開鍵作成部13内のgの2²⁵⁶のpを法とする剰余記数部である。132は、同じく法取り出し部である。133は、同じく乗算部である。134は、同じく割算部である。以下、上記各部の作用等について説明する。秘密鍵作成要求受付部11は、各ユー

ザ3~6(本図ではユーザA)からの固有の秘密鍵の作成要求を、ユーザのキーボードを使用しての操作等で受け付ける。秘密鍵発生部12は、秘密鍵作成要求受付部11が受け付けた要求をもとに、内蔵する乱数発生プログラムにより2進数の乱数を発生させ、これを当該ユーザの秘密鍵とする。なお、本実施例では、乱数の発生に際しては、同一の乱数発生を万が一にも防止し、併せて整理の都合もあるため当該ユーザの公開デジタル通信網上での識別番号をも組み込んだものとしている。またこのため、乱数はpと同じく512ビットとしている。公開鍵作成部13は、2進乱数発生部12の発生させた乱数をもとに公開鍵を作成する。なお、この手順は、後で詳しく説明する。

【0073】公開鍵公開部14は、公開鍵作成部13の作成した公開鍵をその作成要求をなしたユーザ名と共に、全ユーザに公開する。これは、通信網が正当性を承認したユーザ名との公開鍵を対応して登録し、ROM等で発行し、また各ユーザの問い合わせに回答する。秘密鍵通知形態作成部15は、各ユーザの秘密鍵をその操作ミスで外部へ漏出しないよう保護する。秘密鍵通知部16は、秘密鍵を共有鍵の作成等の必要に応じて使用しうるようにする。

【0074】次に、公開鍵作成部13による公開鍵の作成について説明する。公開鍵作成部13は、 g の 2^n 乗の p を法とする剰余記憶部131と法取り出し部132と、乗算部130と割算部134とを有する。 g の 2^n の n を法とする剰余記憶部131は、 g 、 g^2 、 g^4 、 g^8 、…等 g の 2 の累べき乗の p を法とする剰余 g_1 、 g_2 、…、 g_1 をあらかじめ計算して、ROMに記憶している。これを小さい数に例にとって、具体的に示す。 $p=11$ 、 $g=2$ ならば、 $i=\lceil \log_2 11 \rceil=3$ となり、 $2^3 < 11$ となるため、 g 、 g^2 、 g^4 として2、 2^2 、 2^4 を、更に対応する g_1 、 g_2 、 g_4 として2、4、5を記憶している。法取り出し部132は、秘密鍵発生部12から2進数で表現された秘密鍵の通知を受けると、その値で1が立つ桁に対応する g_1 、 g_2 、…、 g_1 を取り出す。これも、小さい数に例にとって具体的に示す。今 $x=101$ (10進の5)とする。1位と3位(各、 g の2の0乗と2の2乗)に1が立っている。このため g_1 と g_4 、すなわち2と5を取り出す。乗算部133は、法取り出し部132の取り出した法を掛け合わせる。割算部134は、乗算部133の乗算結果を n で割り、その剰余を求める。上記具体的な数値で示すならば、 $2^{10}=2^2=2 \times 2^4=2 \times 5=10$ (mod 11)となる。そして、この剰余がユーザAの公開鍵とされる。なお、本実施例で g の累べき乗の剰余を採用しているのは、 g^3 、 g^5 等の法を採用するのよりも一般的に処理が速く、演算機等も2進で動作することにあわせたものである。

【0075】次に、署名付きの送信を行うユーザA側の

重要な処理の流れを図8に、重要な構成を図9と図10に示す。図9において、31は r_2 制御部である。32は2進乱数発生部である。33は r_1 演算部である。34は、通信文(m)入力部である。35は、f関数部である。36は、q記憶部である。37は、排除部である。また、331は、 r_1 演算部内のべき剰余記憶部である。また、332は、同じく法取り出し部である。333は、同じく乗算部である。334は、同じく割算部である。351は、f関数部35内の和算部である。352は、同じく、割算部である。371は、排除部37内のq読み出し出力部371である。372は、同じく引き算部である。373は、同じく比較部である。

【0076】図10において、38はSK部である。381は、SK部38内の $k-1$ 演算部である。382は、同じく r_2+1 演算部である。383は、同じく $r_2 \times x_1$ 演算部である。384は、同じく $r_2+1+r_2 \times x_1$ 演算部である。385は、同じく、S計算部である。以下、上記各部の作用等について説明する。

【0077】最初、システムパラメータの入手(a1)と秘密鍵等の作成操作(a2)がなされ、秘密鍵の作成及び公開鍵の登録がなされる(a3)。 r_2 制御部31は、署名通信発信に当たり、2進乱数発生部32とm入力部34の作用を調整、制御し、後に説明するが、必要な繰り返し処理をも行う。通信文入力部34は、署名発信のための文、例えば「私は、特発 証明です。電話番号は03-3581-1101。確認願います。」等の文書をユーザにより入力され、これを数値(m)化する(a4)。

【0078】2進乱数発生部32は、コミットメント作成のため署名発信毎に相異なる乱数を発生をさせる。またこのため、発信日時等も乱数発生に使用される。(a5)

r_1 演算部33は、発生された2進乱数kをもとに $r_1 \equiv g^k \pmod{p}$ の演算により、 r_1 を求める。このため、通信網提供者における g の 2^n の p を法とする剰余記憶部331、法取り出し部332、乗算部333、割算部334と同じ構成作用をなす剰余記憶部331、法取り出し部332、乗算部333、割算部334を有している。(a6)

f関数部35は、 r_1 演算部33で作成された r_1 と通信文入力部34で数値化された通信文mをもとに、メッセージマスキング法を使用し、 $r_2 \equiv f(r_1, m) \pmod{p}$ の演算を行い、 r_2 を求める。(a7)

このため、 \pmod{p} 上での $r_2 \equiv r_1 + m$ の和算を行う和算部351と、和の p を法とする剰余を求めるための p での割算を行う割算部352とを内蔵している。

【0079】q記憶部36は、あらかじめ別途ユーザにより入力された g をメモリーに記憶している。排除部37は、f関数部35から入力された r_2 とqとの大小比較を行い(a8)、 r_2 がq以上となれば、前述の冗長

攻撃を回避すべくこの送信を行わず、この旨 r_2 制御部31に通知する。

【0080】この通知を受けた、 r_2 制御部31は、2進乱数発生部32に再度異なる乱数発生をなして、(a9) 先の r_1 と異なる r_1 を得、これと通信文入力部34に入力されている通信文 m とで f 関数を部35に f 関数作用させ m 、先と異なる r_2 を求め、更に q との大小比較を行わめめるというプロセスを、 $g-r_2$ が正となるまで繰り返して実行させる。また、 $q-r_2$ が正となれば、この r_2 をSK部37へ出力する。またこのため、排除部37は、 q 読み出し部371と引き算部372と比較部373とを内蔵している。 q 読み出し部371は、 r_2 の入力があると q 記憶部36から q の値を読み出し、引き算部372に通知する。引き算部372は、通知された q から r_2 の引き算を行う。比較部373は、引き算部372の求めた差が0より小ならば r_2 制御部31へこの旨通知すること、この値が正となるまで上述の手順を繰り返して実行されることとなる。また、 r_2 が正ならば、入力された r_2 をそのままSK部へ通知する。

【0081】SK部38は、署名式 $sK \equiv (r_2 + s + 1) + r_2 \cdot x_2 \pmod{p}$ の演算により、送信対象となるメッセージを作成する (a10)。図14に示すような構成である。そして、内蔵している $k-1$ 演算部381は、2進乱数発生部381にて発生された、そしてそれを使用して計算した r_2 の値が q 未満という要件を充たすこととなった乱数 k から1を引き去る。なお、この差を a とする。

【0082】同じく、 $r_2 + 1$ 演算部37は、入力された r_2 に1を加える。同じく、 $r_2 \cdot x_2$ 演算部383は、排除部37から入力された r_2 と図示しない秘密鍵記憶部から入力された x_2 との積を求める。 $r_2 + 1 + r_2 \cdot x_2$ 演算部384は、 $r_2 + 1$ 演算部382から入力された $r_2 + 1$ と $r_2 \cdot x_2$ 演算部383から入力された $r_2 \cdot x_2$ との和を求める。なお、この和を b とする。 s 計算部385は、 $k-1$ 演算部381が求めた a と $r_2 + 1 + r_2 \cdot x_2$ 演算部384が求めた b とを使用して、 $s \cdot a \equiv b \pmod{q}$ を充たす s をユークリッドの互除法により求める。そしてこの結果を図示しない送信部へ送る。

【0083】以上のもので、署名を求める他のユーザBへ、(r_2 , s) が署名文として送信されることとなる。(a11)

図11は、署名文を受信したユーザ側の重要な処理の流れを示す図であり、図12は構成図である。本図において、41は受信部である。42は、拒絶部である。43は、 q 記憶部である。44は、 y_A 記憶部である。45は、 r_2 記憶部である。46は、 s 記憶部である。47は、 g 記憶部である。48は、 $r_2 + s + 1$ 演算部である。49は、 $y_A^{1/S} \pmod{p}$ 演算部である。410

は、 $g^S \pmod{p}$ 演算部である。411は、 $y_A^{r_2/S} \pmod{p}$ 演算部である。412は、 $g^{(r_2+1+S)/S} \pmod{p}$ 演算部である。413は、 $r_1 \equiv g^{(r_2+1+S)/S} y_A^{r_2/S} \pmod{p}$ 演算部である。414は、 f^{-1} 関数部である。

【0084】受信部41は、認証を求める他のユーザ、今Aとする、からの送信文 (r_2 , s) を受信する (b1)。拒絶部42は、受信があった場合、 $r_2 - q$ を計算し (b2)、正なら一応正当なものとして続行する処理を行うべく他部にこの受信文を流すが、正でなければこの署名を拒否する (b3)。またこのため、送信側ユーザと同じく q 記憶部43にあらかじめ q を記憶している。 y_A 記憶部44は、通信網提供者より公開された y_A を、あらかじめメモリーに記憶している。

【0085】 g 記憶部47も、同じくあらかじめ g を記憶している。 r_2 記憶部45は、拒絶部42が一応認証した r_2 を記憶し、 s 記憶部46は同じく s を記憶する。なお、 r_2 と s の区分けは、別途定めた通信規約に基づきなされる。 $r_2 + s + 1$ 演算部48は、 r_2 記憶部45と s 記憶部46からそれぞれ r_2 と s を読み出し、和算で $r_2 + s + 1$ を求める。 $y_A^{1/S} \pmod{p}$ 演算部49は、 y_A 記憶部44から y_A を、 s 記憶部46から s を読み出して $y_A^{1/S} \pmod{p}$ を演算する。 $g^S \pmod{p}$ 演算部410は、 s 記憶部46から s を、 g 記憶部47から g を読み出して、 $g^{1/S} \pmod{p}$ を演算する。 $y_A^{r_2/S} \pmod{p}$ 演算部411は、 r_2 記憶部45から読み出した r_2 と $y_A^{1/S} \pmod{p}$ を演算部49から読み出した $y_A^{1/S} \pmod{p}$ をもとに、 $(y_A^{1/S})^r = r_2$ 乗し、更にこの p を法とする剰余を求める。 $g^{(r_2+1+S)/S} \pmod{p}$ 演算部412は、 $r_2 + s + 1$ 演算部418から $r_2 + s + 1$ を読み出し、 $g^{1/S} \pmod{p}$ 演算部410から読み出した $g^{1/S} \pmod{p}$ を $r_2 + s + 1$ 乗し、更にこの p を法とする剰余を求める。

【0086】 $r_1 \equiv g^{(r_2+1+S)/S} y_A^{r_2/S} \pmod{p}$ 演算部413は、 $y_A^{r_2/S} \pmod{p}$ 演算部411の演算結果と $g^{(r_2+1+S)/S} \pmod{p}$ 演算部412の演算結果とから、 $r_1 \equiv g^{(r_2+1+S)/S} y_A^{r_2/S} \pmod{p}$ の演算により、 r_1 を求める (b4)。 f^{-1} 関数部414は、関数 f^{-1} を使用して演算 $r_2 - r_1$ を行い、 m を求める (b5)。

【0087】以上の構成により、ユーザBはユーザAの送信文から m を入手するが、この際通信網提供者が公開した y_A に相当する秘密鍵 x_A を知っているのはユーザAのみであり、またこの x_A を使用しない限り y_A を使用しての正しい復号もなしえない。このため、送信者は、確かにユーザAの署名であると確認する (b6)。次に、以上の説明とかなり重複するが、以上の手順における通信文の処理、各種の数式をもとにして、式や数値で表現されたデータの変化の様子を中心として、この

手順を説明する。

【0088】図1は、この数値式や面で表現した手順の基本的な構成を示すものである。以下、本図を参照しながら実施例の手順を説明する。

(1) センターによる初期設定

p を素数とし、GF(p) の元を g としその位数を q とする。ここで $p \sim q$ とする。

【0089】GF(p) × GF(p) から GF(p) への写像 f を、 $f(r_1, m) = r_1 + m \pmod{p}$

f の逆写像 f を

$f^{-1}(r_1, f(r_1, m)) = m \pmod{p}$

とし、 $Zq \times Zq \times Zq$ から Zq への写像 h_a, h_b, h_c を、 $h(r_2', s, 1) = s$, $h(r_2', s, 1) = r_2'$ とし、

$h(r_2', s, 1) = r_2' + s + 1 \pmod{q}$

で定義する。また署名式を

$h(r_2', s, 1)k = h(r_2', s, 1) + h(r_2', s, 1) \times y_A \pmod{q}$

で定義する。

【0090】センターは、システムパラメータとして p, q, g, f, h_a, h_b, h_c を公開する。この状態が、図6に示すものである。

(2) ユーザによる署名送信のための秘密鍵の作成及びセンターが認めた公開鍵の登録。

【0091】ユーザAが、メッセージ復元型署名通信を行うため、その秘密鍵を基に公開鍵を作成し、これを通信網提供者が正しいものとして登録する要求を行う。この要求のため、ユーザAはその端末識別番号を使用して乱数を発生させ、秘密鍵 x_A を生成する。次いで、その公開値 $y_A = g^{x_A} \pmod{p}$ を生成し、生成した公開値はセンターを通じて各ユーザに通知される。

(3) ユーザAによる署名の生成及び送付

1. 2進乱数 k を、プログラムによって生成する。

【0092】2. 以下の演算を順に行う。

2-1) $r_1 = g^k \pmod{p}$,

2-2) $r_2 = f(r_1, m) \pmod{p} \cdots (c)$ とする。

2-3) $q \nmid r_2$ の場合、再度上記1)に戻り、異なる2進乱数を生成する。

2-4) $sk = (r_2 + s + 1) + r_2 x_A \pmod{q} \cdots (d)$ より s を計算する。

【0093】3. 上記2)で生成した (r_2, s) をユーザBに送信する。

(4) ユーザBによる受信したメッセージの復元

1. $q \nmid r_2$ ならば、署名を拒絶する。

2. $r_1 = g^{(r_2 + s + 1) / y_A} \pmod{p}$ を計算し、 $f^{-1}(r_1, r_2) = m \pmod{p}$

を計算することにより、メッセージ m を復元する。

【0094】次に、以上の署名の前攻撃性について説明する。以上の構成のメッセージ復元型署名の場合、コミットメント r_1 が従来例の式(a)のように直接平文 m に関与するのではなく、写像 f を通じて関与している。この写

像 f が

(*)1: $GF(p) \ni g, y_A$ 及び m 並びに $Zq = \{0, 1, \dots, q-1\} \ni t, j$ 及び e に対し、 $f(g^t y_A^j, my_A^e)$ 及び $f(g^t y_A^j, my_A^e)$ において、3変数 t, j, e が2個の代数式で非置換である。このため、recovery equation 攻撃を受けない。

【0095】2: $GF(p) \ni r_1, r_2, m, g$ 及び y_A に対し、 $r_2 = f(r_1, m)$ の逆像を $m = f^{-1}(r_1, r_2)$ で定義するとき、任意の2変数関数 ϕ, ψ に対して $f^{-1}(r_1/g, r_2) = \phi(m, g)$ 及び $f^{-1}(r_1/y_A, r_2) = \psi(m, y_A)$ となることから、宮地らにより提案された3つの攻撃(recovery-equation attack, using g and y_A , and homomorphism attack)を回避できる。

【0096】また上記実施例のように構成されたメッセージ復元型署名の場合、従来例の式(b')のように署名式の係数(a, b, c)が $(r_2', s, 1)$ の置換という形ではなく、写像 h_a, h_b, h_c を用いて決定されている。この写像 h_a, h_b, h_c が $(**)(r_2', s = Zq \text{ の元とすると、予め固定された少数値をのぞく全ての } rr_2', ss \text{ に対して、次の二つの条件}$

1. $h(r_2', s, 1) = h(rr_2', ss, 1)$, $h(r_2', s, 1) = h(rr_2', ss, 1)$ のとき $hb(r_2', s, 1) - ha(r_2', s, 1) \neq hb(rr_2', ss, 1)$

2. $h(r_2', s, 1) = h(rr_2', ss, 1)$, $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき $hc(r_2', s, 1) - ha(r_2', s, 1) \neq hc(rr_2', ss, 1)$ を満たすことから、宮地らにより提案された2つの解読(signature-equation attack using g and y_A) を回避できる。さらにこの署名式は従来から存在する比例関係を用いた解読に対しても、署名式が2項に分解されることがないので強い。

【0097】なお、従来から存在する比例関係を用いた比例攻撃に付いては、L.Harn and Y. Xu, "Design of generalised ElGamal type digital signatures schemes based on discrete logarithm", Electron. Lett., Vol. 30(1994), 2025-2026. に詳しい。また、上記実施例のように $p \sim q$ とすることにより、 r_2 の値を制限するステップ(署名生成ではステップ2-3, メッセージ復元ではステップ1)を付加することができる。これにより宮地により提案された1つの解読(redundancy attack)を回避できる。更にこの場合、qのpに対する比が従来のごとく 2^{-400} と小さくなく、 $1/3, 1/2$ することにより、再度乱数を発生させ繰り返しての処理を行わねばならない確率も低下しえる。

【0098】なお、上述の実施例は f を $r_1 + m$ として行ったが、これは勿論他の写像 f で、(*) を満たすものなら何でもよい。またこの際、 $r_1 + m$ のように計算量が小さい写像にすることが望ましい。ha, hb, hc に関しても、上記の性質(**)をもつものなら何でもよい。またこの際、従来から存在する比例関係を用いた解読に対しても強くなるように、さらに計算量が小さい写像にすることが望ましい。

【0099】また、上記の従来例以外のどんなメッセージ復元型署名にも上記の写像を付加すると同様に解読が回避できる。また、上記の署名方式は、メッセージ m に署名する代わりに、 m に1SOで定められたRC 4、RC 2等のハッシュ関数を施したハッシュ値に対して署名し、署名をメッセージとともに送り、ハッシュ値が正しく復元されることをチェックすることで署名を確認するという署名方式としても用いることができる。

【0100】また、上記署名方式は、各ユーザの秘密鍵等は、通信網提供者又はユーザ用の情報発行センターが生成するものとしたが、これは勿論各ユーザが任意にその秘密鍵を選定し、公開値等のみセンターへ登録するようにしてもよい。更に、通信網提供者とユーザ用の情報発行センターが異なってもよい。また、上記署名方式では、各種演算は $GF(p)$ 上でなされるものとしたが、これは勿論 $GF(p^r)$ 上でなされてもよい、この場合には、上記実施例における $(\text{mod } p)$ での演算は $(\text{mod } p^r)$ での演算となり、このため、 r_1 と m を $GF(p^r) \times GF(p^r)$ から $GF(p^r)$ へ字像 f_1 を用いて変換した後、この値を更に $GF(p^r)$ から有限環 $Z_{p^r} = \{0, 1, \dots, p^{r-1}\}$ への変更をなす等の手順が付加される。

【0101】なお、この写像 π は、 $\{a_1, a_2, \dots, a_r\}$ を $GF(p^r)$ の $GF(p)$ 上の基底とすると、 $GF(p^r)$ の元 $x = x_1 a_1 + \dots + x_r a_r$ ($x_1, x_2, \dots, x_r \in GF(p)$)に対して $\pi(x) = x_1 + x_2 p + \dots + x_r p^{r-1}$ で定義される。この手順を図13に示す。(注、上記実施例は $r=1$ の場合であり、 π は恒等写像となり、表面上でここの。(第2実施例)本実施例は、本発明に係るメッセージ復元型署名方式として、楕円曲線上での演算を行うものである。

【0102】本実施例も、基本的な構成、原理は先の第1実施例と異ならない。ただし、有限体 $GF(p)$ 上の離散対数問題の困難性でなく、楕円曲線 $E(GF(p))$ 上の困難性を利用するため、これに関係する点異なる。このため、この相違する点を中心に説明する。デジタル公開通信網における通信網提供者1、各ユーザ3〜6の接続状態及び初期設定としてのシステムパラメータの概略の構成を図14に示す。

【0103】システムパラメータとして $E(GF(p))$ と、 g に換えての $E(GF(p))$ 上の零元と異なる元 G が加えられ、 p は10進30桁の素数である。これは、 $E(GF(p))$ 上の離散対数問題は有限体 p でそれと比べてはるかに困難であることによる。 q が n だが、これは、 G の位数は零元を除き常に p であることによる。また、楕円曲線を使用するため、 f は x 座標関数である。

【0104】各部の構成であるが、第1実施例では、 p を法とする g^k の剰余を計算するため通信網提供者1及

びユーザ側の剰余記憶部131、231等には、 g, g^2, g^4, \dots, p を法とする剰余があらかじめ記憶されていたがこれに換えて、 $G, 2G, 4G, \dots$ が記憶されているのが大きく異なる。更に、これにあらわして、各種の演算部の乗算も足算を行う点も異なる。

【0105】図15に、通信網提供者の公開鍵作成部213の内部構成を示す。本図に示すように、剰余記憶部2131は、 $G, 2G, 4G, 8G, \dots$ をあらかじめ計算して記憶おり、第1実施例の乗算部13と割算部134に換えて足算部2133を有している。また、これにより、公開鍵として、 $E(GF(p))$ 上の点 $Y_A = (X_A, G)$ を計算し、公開する。

【0106】図16に、署名通信を行うユーザA側の構成を示す。本図においては、32は2進乱数発生部であり、34は、通信文入力部であり、これらは、先の第1実施例と異ならない。233は R_1 演算部であり、2進乱数発生部32で発生させた乱数 k 回だけ G を加えた値 kG を求め、その値 R_1 を出力する。このため、あらかじめ、 $2G, 4G, 8G$ に対応する G_2, G_4, G_8 等を記憶している剰余記憶部2331、2進乱数 k の1の立つ桁を取り出す法取り出し部2332、取り出した桁に対応する剰余記憶部2331内の G_1 (ここには2の乗べき)を取り出し、足し算を行う足し算部2333を内蔵している。

【0107】235は、 F 関数であり、 $r_2 = m/x$ (R_1) $(\text{mod } p)$ の演算により r_2 を求める。ここに $x(R_1)$ は R_1 の X 座標値である。238は、求められた r_2 と上記乱数 k をもとに、演算 $s k = (r_2 + s + 1) + r_2 x_k (\text{mod } p)$ より s を求めるSK部である。このため、 $k-1 (=a)$ を求める $k-1$ 演算部2381、 $r_2 + 1$ を求める $r_2 + 1$ 演算部2382、 $r_2 x_k$ を求める $r_2 x_k$ 演算部2383、 $r_2 + 1 + r_2 + x_k (=b)$ を求める $r_2 + 1 + r_2 + x_k$ 演算部2384、式 $s \cdot a = b (\text{mod } p)$ より s を求める s 計算部2385を内蔵している。

【0108】なお、 mod 演算の法が、 q でなく p であるのが第1実施例と大きく異なる。図17は、受信側ユーザの構成図である。本図において、受信部41、 r_2 記憶部及び s 記憶部46は第1実施例のものとは異なる。247は、あらかじめ G を記憶している G 記憶部である。244は、 Y_A をあらかじめ記憶している Y_A 記憶部である。

【0109】248は、 r_2 と s から $(r_2 + s + 1)/s$ を求める $(r_2 + s + 1)/s$ 演算部である。249は、 r_2/s を求める r_2/s 演算部である。2411は、 $E(GF(p))$ 上での演算 $r_2/s Y_A$ を行う $r_2/s Y_A$ 演算部である。2412は、同じく $E(GF(p))$ 上での演算 $((r_2 + s + 1)/s) G$ を行う $((r_2 + s + 1)/s) G$ 演算部である。2413は、同じく、 $E(GF(p))$ 上での演算 $R_1 = ((r$

$2 + s + 1) / s) G + (r_2 / s) Y_A$ を行って R_1 を求める演算部である。2414は、演算 $m = x(R_1) r_2$ (ここに、 $x(R_1)$ は $E(GF(p))$ 上の r_1 の X 座標値) より m を求める m 演算部である。

【0110】このため、 q と r_2 の大小比較を行う構成がないのも第1実施例と異なる。次に、以上の手順におけるデータそのものの処理、数式、演算を中心とした処理の流れを図18に示す。

(1) センターによる初期設定

10進30桁の素数 p とし、 $GF(p)$ 上の元の個数が p となる楕円曲線を E とし、 $E(GF(p))$ の元を零元以外以外の元を G とする。このときその位数は p となる。

【0111】 $GF(p) \times GF(p) \times GF(p)$ から $GF(p)$ への写像 h_a, h_b, h_c を、 $h_a(r_2', s, 1) = s$, $h_c(r_2', s, 1) = r_2'$ とし、

$$h_b(r_2', s, 1) = r_2' + s + 1 \pmod{p}$$

で定義する。また署名式を

$$h_a(r_2', s, 1)k + h_b(r_2', s, 1) + h_c(r_2', s, 1)x_A \pmod{p}$$

で定義する。

【0112】センターは、システムパラメータとして p 、 $E(GF(p))$ 、 G 、 h_a 、 h_b 、 h_c を全ユーザに公開する。

なお、かかる $E(GF(p))$ の作成手順は、別途本願出願人が前掲の特願平6-134339号等にて開示している技術であるため、その説明は省略する。(2) 署名送信を欲するユーザAによるそのための秘密鍵の作成及びセンターが認許した公開鍵の登録。

【0113】ユーザAから、メッセージ復元型署名通信を行うため、その秘密鍵を基に作成した公開鍵を通信網提供者に正しいものとして登録する要求がなされる。このため、ユーザAは、乱数を発生させ、これを自分の秘密鍵を x_A とし、対応する公開鍵を楕円曲線 $E(GF(p))$ 上での演算 $y_A = x_A G$ により求め、これをセンター経由で全ユーザに公開する。

【0114】併せて秘密鍵 x_A は、ユーザAが自分のみ秘密に保持するものとする。

(3) ユーザAによる署名の生成

ユーザBに署名発信を行おうとするユーザAは、以下の処理を行う。

1. 乱数 k を生成する。

2. 2進数の乱数 k を生成する。なお、この乱数は、各送信毎に異なる値が得られるものとしている。

【0115】2-1) $E(GF(p))$ 上で、演算 $R_1 = kG$ により、 R_1 を作成する。

2-2) 法 p 上の演算 $r_2 = m / x(R_1) \pmod{p}$ により、 r_2 を求める。ここに、 $x(R_1)$ は、 $E(GF(p))$ 上の点 R_1 の x 座標値である。…(e) とする。

2-3) 法 p 上の演算 $sk = (r_2 + s + 1) + r_2 x_A \pmod{p}$ …(f) より s を計算する。

【0116】3. (r_2, s) をユーザBに送信する。

(4) 受信したユーザBによるメッセージの復元

1. ユーザAからのメッセージ (r_2, s) を受信したユーザBは $((r_2 + s + 1) / s)G + (r_2 / s)Y_A = R_1$ を $E(GF(p))$ 上で計算し、 R_1 を求める。

【0117】2. 次に、 $m = x(R_1)r_2$ を計算することにより m を得る。上記実施例のように構成されたメッセージ復元型署名の場合、コメントメント R_1 が従来例の式(a)のように直接平文 m に関連するのではなく、式(e)のように x 座標を通して関与している。すなわち、 $r_2 = F(R_1, m) = m / x(R_1)$ となる。この F 関数が

(*)1: $GF(p) \ni g, y_A, m, Z_q = \{0, 1, \dots, q-1\} \ni t, j, e$ に対し、 $F(tg + jY_A, m \times x(eY_A))$ 及び $F(tg + jY_A, m \times x(eG))$ において、3変数 t, j, e が2個の代数式で非置換(置き換えられない)。すなわち、 $m \times (eY_A)$ 、 $m \times (eG)$ の偽造攻撃を受けない。

【0118】2: $E(GF(p)) \ni R_1, G, Y_A, GF(p) \ni r_2, m$ に対し、 $r_2 = F(R_1, m)$ の逆像を $m = F^{-1}(R_1, r_2)$ で定義するとき、任意の2変数関数 ϕ, ψ に対して $F^{-1}(R_1 - G, r_2) \neq \phi(m, G)$ 及び $F^{-1}(R_1 - Y_A, r_2) \neq \psi(m, Y_A)$ となるを満たすことから、宮地らにより提案された3つの解読(recovery-equation attack using g and y_A , and h morphism attack)を回避できる。

【0119】また上記実施例のように構成されたメッセージ復元型署名の場合、従来例の式(b')のように署名式の係数 (a, b, c) が $(r_2', s, 1)$ の置換した形ではなく、写像 h_a, h_b, h_c を用いて決定されている。この写像 h_a, h_b, h_c が $(**)(r_2', s \in Z_q)$ の元とするとき、予め固定された少数値をのぞく全ての rr_2', ss に対して、次の二つの条件

1. $h_a(r_2', s, 1) = h_a(rr_2', ss, 1)$, $h_c(r_2', s, 1) = h_c(rr_2', ss, 1)$ のとき $h_b(r_2', s, 1) - h_a(r_2', s, 1) \neq h_b(rr_2', ss, 1) - h_a(rr_2', ss, 1) = h_a(rr_2', ss, 1) - h_b(rr_2', ss, 1)$, $h_b(r_2', s, 1) = h_b(rr_2', ss, 1)$, $h_b(r_2', s, 1) = h_b(rr_2', ss, 1)$ のとき $h_c(r_2', s, 1) - h_a(r_2', s, 1) = h_c(rr_2', ss, 1) - h_a(rr_2', ss, 1)$ を満たすことから、宮地らにより提案された2つの解読(signature-equation attack using g and y_A)を回避できる。さらにこの署名式は従来から存在する比例関係を用いた解読に対しても、署名式が2項に分解されることがないので強い。なお、従来から存在する比例関係を用いた比例攻撃については、L.Harn and Y. Xu, "Design of generalised ElGamal type digital signatures schemes based on discrete logarithm", Electron. Lett., Vol.30(1994), 2025-2026. に詳しい。

【0120】また、上記例のような楕円曲線を用いると G の位数が定義域 $GF(p)$ の p と等しくなるので、実施例1のように r_2 の値を制限するステップを付加することなく、宮地らにより提案された1つの解読(redundancy attack)を回避できる。また、上述の実施例は x 座標を用いたが、これは勿論他の写像で、(*)を満たすものなら何でもよい。この例、例えば y 座標のように x 座標と同じ

ように計算量が小さい写像にすることが望ましい。ha, hb, hcに関しても、上記の性質(**)をもつものなら何でもよい。またこの際、従来から存在する比例関係を用いた解読に対しても強くなるように、さらに計算量が小さい写像にすることが望ましい。

【0121】また、上記実施例では、定義体GF(p)のpとGの位数が等しくなるような楕円曲線を用いたが、通常の楕円曲線を用いてもよい。このときには、第1実施例のように r_2 を制限するステップを付加する必要がある。また、上記の従来例以外のどんなメッセージ復元型署名にも上記の写像を付加すると同様に解読が回避できる。

【0122】また、第1実施例と同じく、メッセージmに署名する代わりに、mにハッシュ関数を施したハッシュ値に対して署名し、署名をメッセージとともに送り、ハッシュ値が正しく復元されることをチェックすることで署名を確認するという署名方式として用いてよい。また、同じく、E(GF(p))でなくE(GF(p^r))で行ってもよい。

【0123】また、ユーザは、その秘密鍵等の生成を通信網提供者にしてもらうようにしてもよい。これは、適当な乱数生成器がないときに便利である。以上、本発明を実施例に基づいて説明してきたが、本発明は何も上記実施例に限定されないのは勿論である。

【0124】
【発明の効果】以上、説明してきたように、本発明は、法をメッセージ復元性を保ちながら、宮地らにより提案されている従来型のメッセージ復元署名に対する6つの解読法を回避することが可能となり、この一方でそのために付加される計算量も無視できる。このため、公開デジタル通信網において、安全なメッセージ復元型署名方式を提供することが可能となり、その実用的価値は大きい。

【図面の簡単な説明】

【図1】本発明に係るメッセージ復元型署名の第1実施例の、数値や式の変換を中心とした構成、処理を示した図である。

【図2】従来の署名、認諾通信の手順の一例である。

【図3】従来のメッセージ復元型署名の構成を示した図である。

【図4】従来の署名、認諾通信に対する公開鍵によるrecovery-equation 攻撃の概略手順を示した図である。

【図5】同じく、redundancy攻撃の概略図である。

【図6】本発明に係るメッセージ復元型署名通信が実施される公開デジタル通信網の概略構成図である。

【図7】上記実施例における、通信網提供者の要部の構成図である。

【図8】同じく、署名通信を行うユーザAの重要な処理の流れを示した図である。

【図9】同じく、署名通信を行うユーザA側の r_2 計算

に係る部分の構成図である。

【図10】同じく、ユーザA側のSK部を中心とした構成図である。

【図11】同じく、署名文を受信したユーザBの重要な処理の流れを示した図である。

【図12】同じく、署名文を受信したユーザB側の要部の構成図である。

【図13】第1実施例の変形例として、GF(p)でなくGF(p^r)を使用した場合の、関数 π によるGF(p^r)から $Z_{p^r} = \{0, 1, \dots, p^{r-1}\}$ への変換手順を示した図である。

【図14】本発明に係るメッセージ復元型署名通信の第2実施例が実施される公開デジタル通信網の概略構成図である。

【図15】上記実施例における、通信網提供者におけるE(GF(p))上での演算を実行するための構成である。

【図16】上記実施例における署名文の発行を行うユーザAの構成図である。

【図17】同じく、署名文を受信するユーザBの構成図である。

【図18】同じく、数、値、式の変換を中心とした構成処理を示した図である。

【符合の説明】

- 1 公開デジタル通信網提供者(各ユーザへの端末情報発行センターを兼ねる。)
- 2 公開デジタル通信網の回線
- 3、4、5、6 公開デジタル通信網に接続されたユーザ
- 11 秘密鍵作成要求受付部
- 12 秘密鍵発生部
- 13 公開鍵作成部
- 14 公開鍵公開部
- 15 秘密鍵通知形態作成部
- 16 秘密鍵通知部
- 31 r_2 制御部
- 32 2進乱数発生部
- 33 r_1 演算部
- 34 通信文入力部
- 35 f関数部
- 36 q関数部
- 37 排除部
- 373 比較部
- 38 SK部
- 385 s計算部
- 41 受信部
- 42 拒絶部
- 43 q記憶部(ユーザB)
- 44 y_A 記憶部
- 45 r_2 記憶部

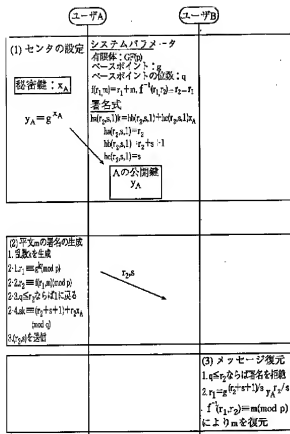
- ```

4 6 s 記憶部
4 7 g 記憶部
4 1 3 $r_1 = g^{(r_2+s+1)/s} y_a^{R_2/\delta} \pmod{p}$ 演算部
4 1 4 f-1 関数部
2 1 3 1 剰余記憶部
2 1 3 3 足算部

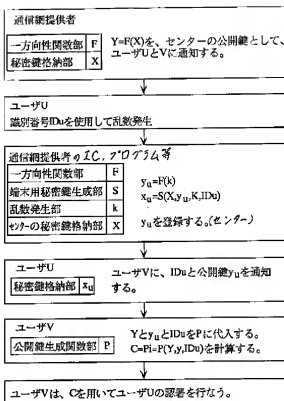
```

- |      |                    |
|------|--------------------|
| 233  | R <sub>1</sub> 演算部 |
| 235  | F関数部               |
| 238  | SK部                |
| 244  | Y <sub>R</sub> 記憶部 |
| 2413 | R <sub>1</sub> 演算部 |
| 2414 | m演算部               |

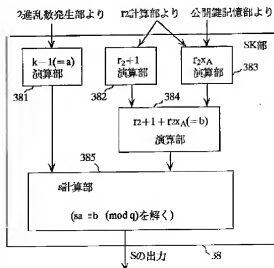
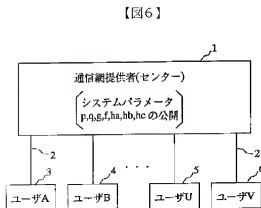
【图1】



【图2】

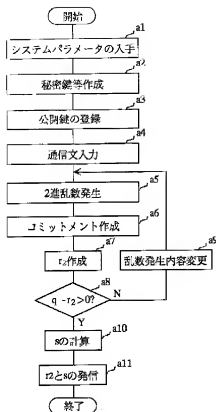


【☒10】

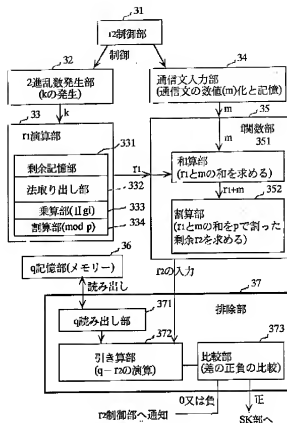




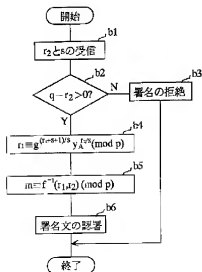
【図8】



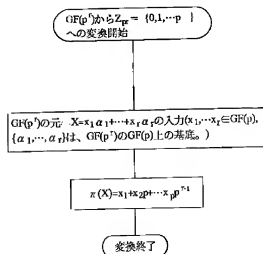
【図9】



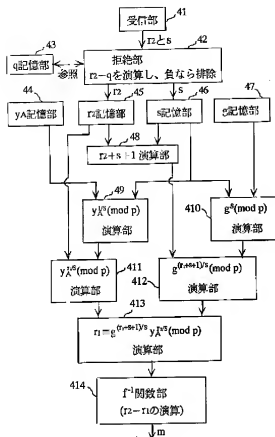
【図11】



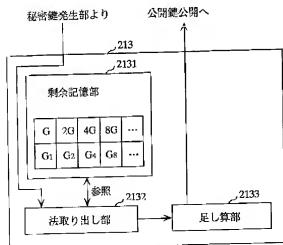
【図13】



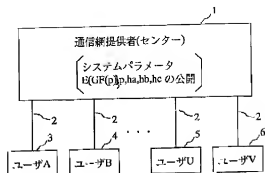
【図12】



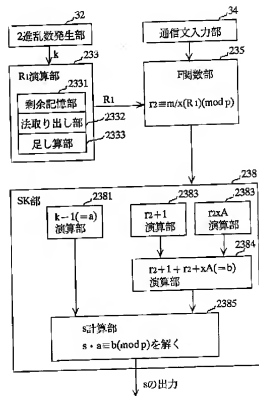
【図15】



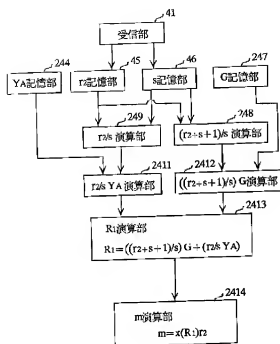
【図14】



【図16】



【図17】



【図18】

